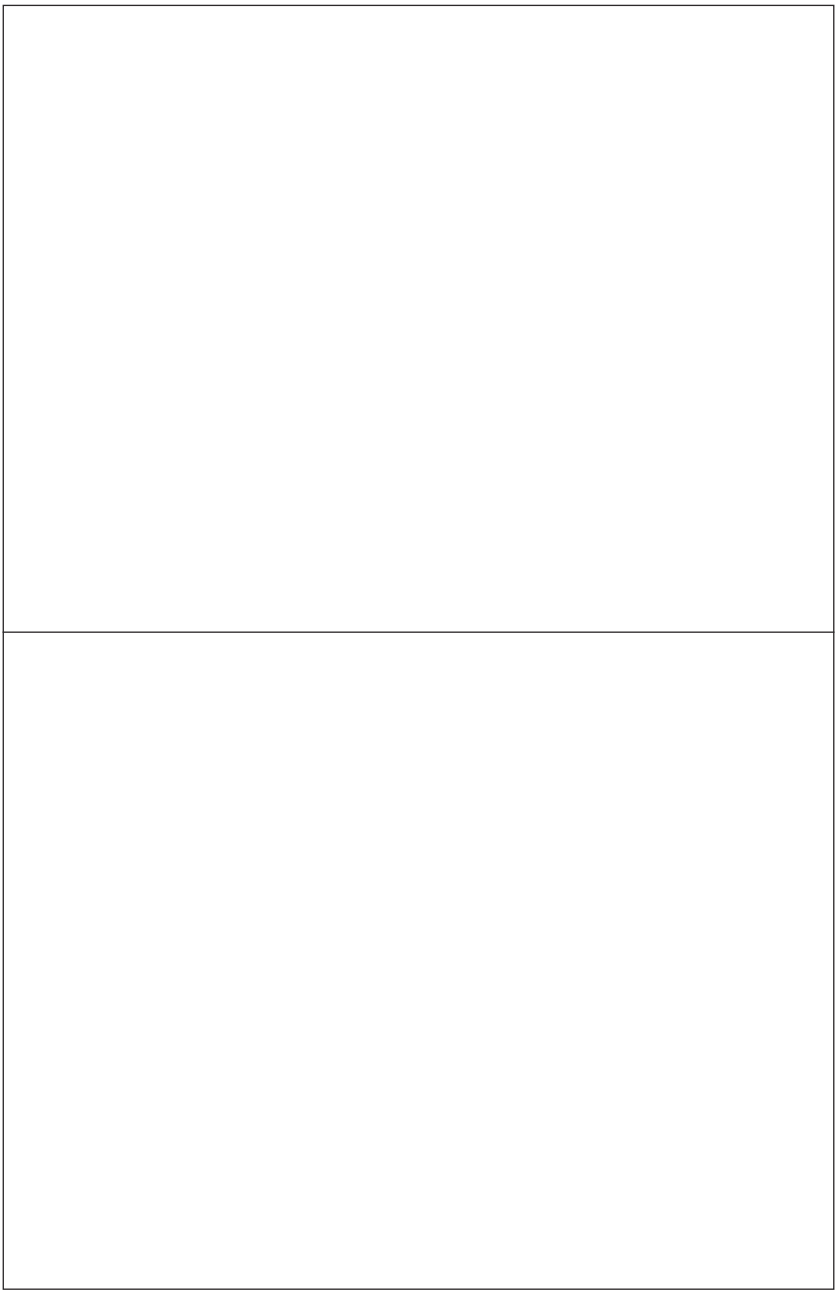
Hans Peter Bull

Netzpolitik: Freiheit und Rechtsschutz im Internet

Nomos

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet



Prof. Dr. Hans Peter Bull

Netzpolitik: Freiheit und Rechtsschutz 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 978-3-8487-0130-8

1. Auflage 2013

Geleitwort

„Freiheit und Rechtsschutz im Internet“ hat Hans Peter Bull sein neues Buch im Untertitel überschrieben. Er spricht damit zwei entscheidende Punkte an, die seit Langem eine wesentliche Rolle in jeder ernsthaften Diskussion um die Zukunft des Internets spielen.

Es sind zwei Welten, die da aufeinander prallen. Viele Nutzer plädieren für Freiheit im Internet ohne Wenn und Aber, wie in der DIVSI-Milieu-Studie nachzulesen ist. Andere verlangen Schutz, fühlen sich unsicher, wollen mehr verbriefte Sicherheit auch durch staatliche Eingriffe. Das hat die zitierte Studie ebenfalls ergeben.

Wie sind diese beiden Extreme einvernehmlich unter einen Hut zu bringen? Denn es ist auf Dauer keine Lösung, sich vor dem dornigen Weg zum Konsens zu drücken. Ein Patent-Rezept gibt es bislang nicht. Immerhin hat die DIVSI-Milieu-Studie dazu beigetragen, diese Thematik endlich nachhaltiger aufzugreifen.

Ich hoffe zuversichtlich, dass auch die Arbeit von Hans Peter Bull die in Gang gekommene Diskussion weiter belebt und intensiviert. Sein Beitrag hat Gewicht. Prof. Dr. Hans Peter Bull, ein anerkannter Hamburger Rechtswissenschaftler, war der erste Bundesbeauftragte für den Datenschutz, war Innenminister in Schleswig Holstein – ein wahrlich aktiver Emeritus, der immer wieder zu Fragen der Zeit Stellung nimmt.

Seine Gedanken zur Netzpolitik werden keineswegs ungeteilten Beifall finden. Beispielsweise dann, wenn er mit einem Fragezeichen versieht, dass „Hacker als Agenten des Fortschritts“ gesehen werden können.

„Die Geheimheit der Privatsphäre des Menschen, die in unserem Kulturkreis seit Jahrhunderten ein wesentlicher Bestandteil seiner Personalität ist, ist neuen Gefährdungen ausgesetzt, die zum Anlass ganz neuer Überlegungen gemacht werden müssen“, hat DIVSI-Schirmherr Prof. Dr. Roman Herzog festgestellt. Hans Peter Bull stellt nicht nur diese geforderten neuen Überlegungen an. Er zieht auch ein Fazit der bisherigen Entwicklungen und riskiert einen Blick in die Zukunft.

Sein Buch passt zu dem, was sich DIVSI zur grundsätzlichen Aufgabe gemacht hat. Wir wollen den Dialog in Gang bringen und mit neuen Aspekten beleben, der am Ende – hoffentlich – zu mehr Vertrauen und Sicherheit im Internet führt. Ich freue mich, dass das DIVSI die Veröffentlichung dieser Schrift unterstützen kann.

Matthias Kammer
Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet

Inhaltsverzeichnis

Vorwort

Kann das Internet die Demokratie und den sozialen Rechtsstaat retten? Oder unterwirft uns die digitale Technik anonymen Mächten und reißt alle tradierten Werte und Ordnungen in den Abgrund? Über die Wirkungen des Internets[1] und des allgegenwärtigen Computers wird viel spekuliert; weithin herrscht Unsicherheit, wie man mit den neuen Techniken politisch und juristisch umgehen soll. „Netzpolitik" ist plötzlich ein Thema nicht nur für Computerfreaks, die von „Freiheit des Internets" reden, sondern auch Gegenstand von Parteitagen, Talkshows und Zeitungskommentaren. Der Deutsche Bundestag hat eine Enquete-Kommission „Internet und digitale Gesellschaft" eingesetzt. Das Verhältnis von Demokratie und Internet wird in Podiumsdiskussionen und Arbeitskreisen erörtert, und es gibt erste Parteitagsbeschlüsse, Programmskizzen und Gesetzentwürfe.

Diese Produkte der beginnenden Debatte enthalten mehr Fragen, allgemeine Versprechungen und Prüfungsaufträge als verlässliche Antworten. Was eigentlich „Netzpolitik" bedeutet und welche Ziele sie verfolgt oder verfolgen sollte, wird selten erklärt;[2] tatsächlich sind es teilweise höchst heterogene Einzelthemen, die unter diesem Dach zusammengefasst werden sollen. Die Meinungsführer in Medien, Wissenschaft und Politik sind schnell darin, philosophische, politische, ökonomische und rechtliche Fragen aufzuwerfen, aber zögerlich bei den Antworten. Soweit sie Behauptungen aufstellen, sind dies oft die großen Welterklärungsformeln, die eher den Ausgangspunkt der Debatte markieren als dass sie genaue Aufklärung oder gar Lösungen enthielten. Wie auch sonst üblich, werden – je nach Standpunkt – die Politiker, die Wissenschaftler, die Medien, die Unternehmen oder ganz allgemein das Volk dazu aufgefordert, sich Gedanken zu machen, sich „der Herausforderung zu stellen", „das Thema ernst zu nehmen" oder sogar „eine Lösung" herbeizuführen. Die Reaktion auf die drängenden Fragen wird jeweils von *anderen* erwartet, und ungeachtet der großen Meinungsverschiedenheiten im Volk werden „die Politiker" in die Pflicht genommen, alles auf einmal für alle überzeugend zu ordnen.

Wir können deutlich mehr Klarheit und auch mehr Lösungsansätze gewinnen, wenn wir die tatsächlichen Verhältnisse genau betrachten und die wahrscheinliche künftige Entwicklung konkretisieren und sodann diese Annahmen mit den zentralen Aussagen der geltenden Verfassungs- und Gesetzesnormen konfrontieren. Die

1 Ich zögere, den Genitiv von „Internet" mit dem Schluss-s zu bilden, aber dieser deutsch-englische Sprachmischmasch wird sich wohl durchsetzen.
2 Ein aktueller Überblick: Holznagel/Schumacher 2011.

folgenden Darlegungen sollen zu solcher Art Klarheit beitragen. Notwendig ist eine „Entmythologisierung des Internets“[3], also jene Ernüchterung, die uns sowohl vor unkritischer Euphorie wie vor apokalyptischen Ängsten bewahrt und damit frei macht für die Wahrnehmung all der Chancen, die uns die neue Technik bietet. Es kommt darauf an, uns als Bürgern und Marktteilnehmern und unseren Repräsentanten in Politik und Wirtschaft zu verdeutlichen, dass das Netz und die ihm angeschlossenen Computer, für sich genommen, moralisch und rechtlich *neutral* sind, also von den Gestaltern und Nutzern geordnet und geregelt werden können und müssen. Das Netz „kümmert sich nicht darum, ob seine Wirkungen gut oder schlecht sind“[4]. Es liegt an den Nutzern, welche Folgen die Einführung des Internets hat, also an uns selbst. Wir aber haben Volksvertreter gewählt, die mit Hilfe der Regierung und ihres Apparats das anzuwendende Recht schaffen und für seine Durchsetzung sorgen sollen. Die Öffentlichkeit nimmt an den rechtspolitischen Debatten lebhaft Anteil, aber es fehlt vielfach an zuverlässigen Informationen und auch an klaren und konsentierten Bewertungsmaßstäben.

Als vor achtunddreißig Jahren, im „Orwell-Jahr“ 1984, mein Buch „Datenschutz oder Die Angst vor dem Computer“ erschien, gab es das Internet noch nicht, aber es gab ähnlich aufregende und beunruhigende Prognosen und Visionen von der weiteren Entwicklung, wie sie heute für das Internet im Schwange sind. Inzwischen hat die Informations- und Kommunikationstechnik tatsächlich riesige Sprünge gemacht, so dass unser damals geschaffenes Instrumentarium zur rechtlichen Einbindung der Computer – das Datenschutzrecht und die Datenschutzaufsichtsbehörden – vielen heute als anachronistisch vorkommt.

Ich meine aber, dass es lohnt, ja dass es unverzichtbar ist, sich auf die langjährige Diskussion über das Verhältnis von Recht und Technik zu besinnen und die Erfahrungen des bisherigen Umgangs mit Computern und Internet intensiver auszuwerten, als dies bisher geschieht. Wir sollten versuchen, von den unbestrittenen Wertaussagen zu den konkreten Gestaltungs- und Bewertungsproblemen vorzustoßen. Für die grundsätzliche (rechtliche, politische und moralische) Bewertung bedeutet es zum Beispiel keinen gewichtigen Unterschied, ob Menschen mit Hilfe des modernsten Computernetzes überwacht oder manipuliert werden oder ob dazu veraltete oder überhaupt keine Technik (sondern etwa ein Netz von Spitzeln und Denunzianten) eingesetzt wird; die Grenzen sind danach zu bestimmen, ob die betroffenen Individualrechte und Interessen etwa ausnahmsweise vor einem höheren Interesse der Allgemeinheit zurücktreten müssen. Allenfalls die Nebenwirkungen der verwendeten Mittel unterscheiden sich und können ihrerseits rechtlich unterschiedlich beurteilt werden.

3 Eisel 2011, S. 25.
4 Nicholas Carr, The amorality of Web 2.0, online unter: www.roughtype.com, 3. Oktober 2005, zitiert nach Eisel 2011, S. 25 f.

So befremdlich das auch den Technikexperten vorkommen mag: Die neue Technik muss aus der Perspektive der alten Werte – also der Grundentscheidungen der Verfassung und der Sozialethik – betrachtet und beurteilt werden. Soweit die Verfassungen keine eindeutigen Ableitungen erlauben, ist die Politik berufen und in der Lage, das Recht weiterzuentwickeln, bestehende Regelungen zu modifizieren und vielleicht auch rechtstechnisch neue Lösungen zu erarbeiten, neue Rechtsfiguren zu kreieren. Aber ein völliger Neuansatz der Rechtsetzung ist weder nötig noch sinnvoll.

In diesem Sinne will ich zeigen, dass es rechtliche Ansätze gibt, mit denen wir der aktuellen Probleme Herr werden können. Klar ist, dass es allein mit Rechtsnormen nicht getan ist, dass also noch andere Methoden nötig sind, um die Risiken der fortschreitenden globalen Vernetzung auszuräumen und die Chancen, die das Netz bietet, angstfrei nutzen zu können. Aber das ist ein anderes Thema.

Einleitung: Das Unbehagen an der Technik und die Macht des Rechts

Die Ausgangslage und die Gegenstände der Diskussion

Dem Internet werden Wirkungen vielfältigster Art zugeschrieben – Veränderungen der sozialen Welt, der Politik, der Wirtschaft und der individuellen Lebensverhältnisse. Das Internet, so heißt es, schafft ganz neue Freiheit(en), erweitert unseren Lebensraum und unser Wissen, vermittelt uns Zugang zu anderen Kulturen, lässt uns am Leben anderer teilnehmen und neue Freundschaften knüpfen, eröffnet neue Geschäftsfelder, formt die politische Willensbildung auf allen Ebenen neu, stärkt also die Demokratie. „Das Internet prägt unser Leben, ob wir wollen oder nicht, ob wir mitmachen oder nicht. Gesellschaft und Wirtschaft funktionieren nicht mehr ohne.“[5] Überall liest man inzwischen, wir lebten in einer „digitalen Gesellschaft“ oder einer „digitalen Demokratie“.

Die Bewusstseinslage ist überdies dadurch kompliziert, dass die einen die Technik als Heilsbringer ansehen, während andere sie als fundamentale Bedrohung unserer Kultur betrachten. Es ist zwar stark übertrieben, einen „digitalen Bürgerkrieg“ zu diagnostizieren, aber von Einigkeit über Segen oder Fluch der Technik sind wir weit entfernt, und es ist nicht abwegig, von einem Zusammenstoß der Kulturen zu sprechen.

Wie ist die Lage wirklich? Was ist damit gemeint, dass „unser Leben“ durch das Internet „geprägt“ werde und dass Gesellschaft und Wirtschaft ohne dieses nicht mehr „funktionieren“? Immerhin haben alle früheren Generationen ohne ein elektronisches Netz kommuniziert, und die sozialen Systeme haben auch damals „funktioniert“. Aus dieser vermeintlich grauen Vorzeit sind uns geistige Schätze überliefert, die nach wie vor die wesentlichen Inhalte aller kulturellen Produktion und Konsumtion ausmachen und neue Kreation anregen. Wer das Internet zum Schlüssel aller gesellschaftlichen Verhältnisse und kultureller Prägung erklärt, hat eine zu enge Perspektive. Gewiss sind Verwaltung und industrielle Produktion von zuverlässiger Informationsverarbeitung abhängig, aber die Lebenssituation der meisten Menschen und die Verteilung von Macht und Wohlstand werden davon nur mittelbar beeinflusst. Wesentlich für den Zustand der Gesellschaft sind ganz andere

5 Fischermann/Hamann 2011, S. 12. Wie das Internet „unser Leben“ und „unser Denken“ „prägt“, wird in zahlreichen Publikationen der letzten Jahre behauptet und mit Beispielen illustriert. Ein Beispiel für alle: Görig 2011. Die Süddeutsche Zeitung bringt u.v.a. eine Doppelseite mit Beiträgen unter dem Titel „Gefangen im Netz“ (17./18.3.2012). Miriam Meckel fragt: „Wie lange unterscheiden wir uns noch vom Computer?“ (Meckel 2012).

Faktoren: die globalen Machtstrukturen, der Zustand der natürlichen Umwelt, die wirtschaftliche Entwicklung der einzelnen Länder, die Arbeitsbedingungen und die Einkommens- und Vermögensverteilung, das Wohnumfeld, die Verkehrsprobleme – und für den Einzelnen nicht zuletzt die unmittelbaren persönlichen Beziehungen zu anderen Menschen.

Die Rede von der „digitalen Gesellschaft" und der „digitalen Demokratie" führt in die Irre. Denn diese Begriffe verweisen ja nicht auf soziale Strukturen, sie bezeichnen vielmehr nur den Umstand, dass wir uns der „digitalen" *Technik* bedienen. Sprachlich ist auch dies fragwürdig. „Digital" bedeutet „ziffernmäßig" und verweist auf die Besonderheit der elektronischen Prozesse, dass sie auf der Umsetzung aller anderen Signale in die Ziffern 0 oder 1 beruhen. Dieses Charakteristikum der elektronischen Informationsverarbeitung ist in der Außenwelt, in den Wirkungen der technischen Prozesse *nicht erkennbar* und hat keine Wirkungen. Wer ständig auf einen Bildschirm schaut, seine Informationen überwiegend aus dem Netz bezieht und seine Kommunikation überwiegend über das Netz laufen lässt, mag sich als „homo reticuli" fühlen.[6] Die meisten Menschen aber leben und denken nicht „digital", sondern nach wie vor als soziale Wesen unter anderen. So halten die Bürger insgesamt „an ihren eingefahrenen Routinen der politischen Kommunikation" fest.[7] Richtiger wäre es, von „Informationsgesellschaft" oder vielmehr „Informationstechnikgesellschaft" zu sprechen. Auch der Ausdruck „Netzwerkgesellschaft"[8] ist passender als „Informationsgesellschaft".

Betrachten wir also das Internet und seine Wirkungen genauer, ohne auf die übersteigerten und irritierenden Vorstellungen der unkritisch Faszinierten hereinzufallen, und zwar zunächst von außen: Wie nutzen wir es? Welche Wirkungen treten ein?[9] Auf diesem Wege können wir eine genauere Vorstellung davon erlangen, welche Vorgänge überhaupt als rechtlich regelungsbedürftig in Betracht kommen. Erst wenn hierüber Konsens besteht, ist es sinnvoll, andere Ansätze – also politische, mediale, pädagogische, ökonomische oder sonstige Einwirkungen auf das Verhalten der Menschen – zu erörtern.

6 Übersetzt also: „Netzmensch", gemeint ist „vernetzter Mensch"; genauer wäre: Mensch des kleinen Netzes, so Kurz/Rieger 2012, S. 7.
7 Emmer/Vowe/Wolling 2011, S. 308.
8 Ihn benutzt Sieber 2012, S. 10.
9 Sehr interessante empirisch begründete Aussagen zur Entwicklung der politischen Online-Kommunikation in Deutschland enthält die Studie von Emmer/Vowe/Wolling: „Bürger online" (2011).

Die Vielfalt der Nutzungen

Beim Surfen im Internet kann man ins Schwärmen geraten. Was wir früher mit großer Mühe in vielen Büchern nachschlagen mussten, kommt heute sofort auf unsere Bildschirme. Wir können uns über die verschiedensten Themen schneller und umfassender informieren als jemals zuvor. Wir vergewissern uns vieler Dinge, die das Gedächtnis unscharf überliefert hat oder über die wir in den „alten" Medien zu wenig finden. Wir erhalten unerwartete Informationen, die unseren Horizont bereichern. Texte aus aller Welt, an die wir früher gar nicht herangekommen sind, werden sekundenschnell greifbar. Wir können uns am Computer hervorragend unterhalten – mit Filmen und Videos aller Art, politischen und unpolitischen Texten und Bildern, mit Geschichte und Geschichten, Science-fiction und Belletristik, und wir können Musik hören und Spiele spielen. Ein phantastischer Komfort!

Auch die E-Mail-Technik ist begeisternd. Ohne sie hätte ich manche Arbeit nicht oder nur viel langsamer fertigstellen können. Ich kann ohne Aufwand eine große Zahl von Empfängern ansprechen, mich in kurzem Takt mit anderen austauschen und streiten. So wird aus einseitiger Information eine mehrseitige Kommunikation. Sogar mit denen, die mir bisher nur etwas gesendet haben, kann ich kommunizieren: Die Rundfunkveranstalter ermöglichen zunehmend (und gewiss künftig noch wesentlich mehr) ihren Rezipienten, aus der passiven Konsumentenrolle zu schlüpfen und sich zu den Sendungen zu äußern, ja daran teilzunehmen.

Viele Millionen Menschen haben sich in „sozialen Netzwerken" eingeschrieben, um mit anderen noch mehr zu kommunizieren. Im „Facebook" nennen sich die auf diese Weise zunächst technisch miteinander Verbundenen „Freunde", im „Twitter" heißen sie „Followers". Ich habe mir Freunde und Korrespondenzpartner auf andere Weise gesucht und brauche die technikgestützten Netzwerke nicht, aber für unzählige Jüngere sind sie zu einem unverzichtbaren Teil ihres Lebens geworden.

Der größte Teil der Menschen in Deutschland hat bereits jetzt die Möglichkeit, PC und Internet zu nutzen und sich an ihren Möglichkeiten zu erfreuen. Die Zahl der Anschlüsse wächst ständig; nach neueren Angaben sind schon vier von fünf Deutschen regelmäßig online, bei den unter 30-jährigen sogar fast alle (98 Prozent)[10]. Mitglieder in sozialen Netzwerken sind angeblich schon vierzig Millionen Deutsche. Die Nachrichten, „tweets", „posts" und wie immer auch die Produkte heißen, sind nicht mehr zählbar; die Schätzungen sind umwerfend, unvorstellbar. Die Unternehmen, die der Allgemeinheit diese Technik zur Verfügung stellen,

10 Davon geht z.B. die Grundlagenstudie „Vertrauen und Sicherheit im Internet" aus, die das Sinus-Institut Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet angefertigt hat (DIVSI 2011, S. 7). Weitere Angaben (u.a. vom BITKOM-Verband) bei Spindler 2012, S. 15 f. mit Fn. 43 f.; ausführliche Analyse der verschiedenen Formen von Mediennutzung auf der Grundlage der ARD/ZDF-Online-Studien: von Eimeren/Frees 2012. S.a. www.ard-zdf-onlinestudie.de.

werden unglaublich reich; sie speichern unbeschreibbar große Datenmengen und werten sie aus, angeblich zum Nutzen der Mitglieder, auf jeden Fall aber zum Nutzen der Werbung treibenden Wirtschaft und damit zu ihrem eigenen Nutzen.

Die Zahl der Internetanschlüsse besagt aber wenig über *Art und Intensität der Internetnutzung* und damit über die Dimensionen der abzuwehrenden Risiken. Ein großer Teil der gemeldeten Nutzer verhält sich keineswegs so aktiv wie die Fans, die ständig im Netz surfen und alles ausprobieren wollen, was angeboten wird. Internet ist ein „Aktivitätsmedium“,[11] aber sehr viele bleiben passiv, manche davon weil es ihnen schwerfällt, sich im Netz zu orientieren, oder weil sie den Zeitaufwand scheuen. Andere sind zwar aktiv, aber streben nicht nach neuen Erkenntnissen und erst recht nicht nach politischer Mitwirkung, sondern wollen sich informieren, Waren und Leistungen bestellen und sich unterhalten, z.B. Videos ansehen oder die Mediatheken der Fernsehsender besuchen.[12] Die Idealisten, die andere Prioritäten setzen, schließen von sich auf alle anderen und schaffen sich damit ein falsches Bild von der Lebenswirklichkeit der Vielen. Allgemeine Regeln sind auf die normalen, typischen Fälle abzustellen; Ungewöhnliches, Besonderes kann und muss bei der Rechtsanwendung im Einzelfall berücksichtigt werden.

Die Problemfelder im Einzelnen: Individualrechte und Allgemeininteressen

Vor diesem Hintergrund sind es bestimmte Risiken der Techniknutzung, die rechtspolitisch vorrangig behandelt werden müssen. Es sind diejenigen Phänomene, die den Betroffenen Angst machen oder von Experten als bedrohlich bezeichnet werden (was nicht unbedingt dasselbe ist). Dabei sollten wir sowohl die Bedrohung von Individualrechten wie die Gefahren für das Allgemeinwohl betrachten. Die Einzelnen fürchten vor allem um die Bewahrung ihrer Privatsphäre und ihrer Geheimnisse und um die Sicherheit und Unbefangenheit der Kommunikation. Sie wollen nicht beobachtet werden, und sie wollen ihre Entscheidungsfreiheit behalten. Es geht um die Unbefangenheit der Kommunikation, um die Abwehr von Überwachung, „Verdatung“ und Manipulation. Mit der Entstehung des weltweiten Netzes ist das Interesse der Nutzer hinzugekommen, sich im Netz frei zu „bewegen“, sich überall zu informieren, alle gespeicherten Inhalte ungehindert und möglichst unentgeltlich zur Kenntnis zu nehmen und die eigenen Botschaften ungehindert zu verbreiten. Dabei entstehen Konflikte mit anderen, die das Gleiche wollen oder aber gerade nicht wollen, dass Dritte ihnen „ins Gehege kommen“.

11 Eisel 2011, S. 41.
12 Einzelheiten des Nutzungsverhaltens u.a. bei von Eimeren/Frees 2012.

Richtig verstandene Netzpolitik greift darüber weit hinaus.[13] Der Staat hat nicht nur Freiheitssphären zu gewährleisten, sondern auch aktiv zum Schutz von Individual- und Gemeinschaftsgütern tätig zu werden. So muss er grundsätzlich (wenn auch nicht immer) gegen illegale Äußerungen vorgehen, strafbare Handlungen bekämpfen (Kinderpornographie ist nur ein Bereich von vielen!), und ganz allgemein Rechtsschutz zur Verfügung stellen, damit der Einzelne sich erfolgreich wehren kann, wenn er von anderen angegriffen, betrogen oder beraubt wird. Er muss einen Grundbestand an Kommunikations-Infrastruktur für die ganze Bevölkerung garantieren und unter Umständen durch Subventionen oder in eigener (bzw. kommunaler) Regie dafür sorgen, dass auch entlegene Teile des Landes an das weltweite Netz angeschlossen werden. Zugangsbarrieren sollen abgebaut werden, so dass jeder und jede sich im Internet informieren und äußern kann. In diesen Zusammenhang gehören auch die Stichworte Netzneutralität und Freiheit der Internetdienste.

Netzpolitik will und muss sich schließlich auch darum kümmern, wie sich die Technisierung auf den Zustand der Gesellschaft auswirkt: Wie verteidigen und entwickeln wir die demokratische Teilhabe und die Grundwerte unserer Kultur, wie sorgen wir für die Bildung der nachwachsenden Generationen? Auch hinter diesen Fragen stehen Konflikte, nämlich Meinungs- und Interessenunterschiede über die richtige Entwicklung des Gemeinwesens. Es geht um Bildung und Ausbildung, um Medienpädagogik und Kulturpolitik. Von rechtlichen Regelungen und ihrer Durchsetzung wird hier niemand allzu viel erwarten; aber ganz unwichtig sind Normen auch auf diesen Feldern nicht.

Dem entsprechen die wichtigsten Themen, die sich bei der praktisch-politischen Bewältigung der Probleme des Internets stellen:

- Internetfreiheit: Gibt es ein „Recht auf Internet“ und was bedeutet es?
- Wirksamer Schutz des Persönlichkeitsrechts und anderer Individualrechte
- Sicherung und Ausgestaltung der Informationsfreiheit
- Urheber- und Leistungsschutzrechte versus Freiheit der Internetnutzung
- Effektuierung des Verbraucherschutzes
- Ausbau der Infrastruktur und Gleichbehandlung bei der Nutzung der Netze

Die zentralen Themen der Netzpolitik werden in den drei Hauptteilen dieser Schrift behandelt: im I. Teil die Rechtsstellung des Individuums (anknüpfend an die drei ersten Punkte der obigen Zusammenstellung), im II. Teil die ökonomische und technische Sicht auf die Konflikte im Internet (insbesondere Urheberrechtsfrage und Verbraucherschutz) und schließlich im III. Teil die – von den Individualrechtsfragen zu trennende – Diskussion über neue Formen der Demokratie. Zu kurz kommen dabei die kultur- und bildungspolitischen und -philosophischen Fragen;

13 Vgl. nur Holznagel/Schumacher 2011.

sie sind hintergründig bedeutsam, aber nicht mehr Gegenstand dieser Schrift. Der IV. Teil befasst sich mit den rechtspolitischen Konsequenzen, also dem, was Netzpolitik bewirken sollte.

Zuvor aber ist zu erörtern, inwieweit Gesetzgebung und Rechtspraxis dazu beitragen können, die Entwicklung in die gewünschte Richtung zu lenken.

Was kann das Recht bewirken?

Wir können uns von der vermeintlichen Macht der Computer befreien – nicht als Maschinenstürmer wie seinerzeit die von der Industrie verdrängten Weber, sondern zum einen durch klugen Umgang mit den neuen Instrumenten,[14] zum anderen indem wir die Menschen, die über die Apparate verfügen, bei deren Verwendung kontrollieren. Eben dies geschieht durch Recht und seine Durchsetzung.

Maßstäbe setzen

Freilich scheinen immer mehr Menschen dem Gesetzgeber zu misstrauen. Nicht nur dass sie von der Politik pauschal nichts Gutes erwarten – sie zweifeln auch an der Wirksamkeit von Rechtsnormen. Dazu besteht auch Anlass; in vieler Hinsicht lässt sich eine Erosion des Rechtsbewusstseins, ein Nachlassen der Rechtsbefolgung beobachten – keineswegs nur im Internet. Gleichzeitig wird jedoch gefordert: „Die Politiker müssen das Netz beherrschen, sonst beherrscht das Netz die Politik“[15]. „Die Politiker“ – das sind die Menschen, die für die Gesetzgebung verantwortlich sind. Gegen alle Politikverdrossenheit und Erosion des Rechts fordert also die Öffentlichkeit – mit Recht –, dass die Entwicklung durch Rechtsnormen gesteuert (oder zumindest beeinflusst) wird. Das Vertrauen in Recht und Staat ist zwar zurückgegangen, und auch die Mitglieder der Zivilgesellschaft vertrauen sich gegenseitig immer weniger. Aber das Vertrauen in die Akteure auf den verschiedenen Ebenen kann durch neues Recht oder die Wiederbelebung alter Rechtsprinzipien wieder gestärkt werden.

Das Recht bewährt sich nicht nur wenn es „durchgesetzt“ wird. Es wirkt selbst dann, wenn viele es nicht befolgen. In Rechtsnormen werden zunächst einmal *Maßstäbe* gesetzt, aus denen Verhaltensregeln für Individuen und Staatsorgane und Beurteilungskriterien für tatsächliche Vorgänge und Zustände hergeleitet werden.

14 Dazu etwa Kurz/Rieger 2012, insbes. S. 247 ff. Ebenso in der Grundlinie Beckedahl/ Lüke 2012.

15 Wefing 2011. Dort auch die weiteren Zitate. In Pham/Wefing 2012 wird jedoch Entwarnung gegeben.

Manchmal bleiben sie latent, aber unter veränderten Umständen werden sie manifest und verändern die Wirklichkeit.

Die Ordnung der Werte

In der Internet- und Computer-Diskussion lässt sich beobachten, dass zwar viel (und oft unkritisch) über die neuen *Möglichkeiten* gesprochen wird, die sich bieten, aber wenig von den *Werten*, deren Verwirklichung man anstrebt. Zwar werden ständig die Grund- und Menschenrechte und die Grundprinzipien der Demokratie beschworen, aber diese Bezugnahme bleibt meist abstrakt, und zu selten wird gefragt, wie diese hohen verfassungsrechtlichen Werte sich zu anderen Wertvorstellungen verhalten, die möglicherweise damit kollidieren könnten. Es fehlt an einer soliden *Werteskala*, an einer Rangordnung der Rechtspositionen, die bei genauer Betrachtung der Problembereiche in den Blick kommen. Gewiss ist es überaus schwierig, eine solche Werteordnung festzustellen, aber wenn ein konkreter Fall zu lösen ist, muss eben dies zwingend geschehen: Die eine Position muss – nach sorgfältiger Abwägung! – hinter der anderen zurückstehen. Typisch für viele aktuelle Diskussionen ist aber, dass Konflikte nicht eindeutig entschieden werden, dass man beide Seiten zufrieden stellen oder zumindest beschwichtigen möchte. Das heißt den Kuchen essen und ihn doch behalten wollen – ein allzu beliebtes Spiel nicht nur in der Politik.

Rechtspolitik muss *Prioritäten* bestimmen, um die stets knappen Ressourcen effektiv und effizient einzusetzen. Wenn für die Lebensmittelkontrolle nicht genügend Geld und Stellen zur Verfügung stehen, kann nicht gleichzeitig mehr Personal für den Schutz von Kundendaten verwendet werden. Wenn die Jugendämter unterbesetzt sind und deshalb potentielle Pflegeeltern nicht auf ihre Eignung prüfen können – wie es offenbar mehrfach geschehen ist; dadurch sind mehrere Kinder ums Leben gekommen –, dann verliert etwa die Forderung nach flächendeckenden Breitbandnetzen an Bedeutung. So wichtig Themen wie die Netzneutralität und die Transparenz der Datenverarbeitung auch sind – es gibt noch wichtigere, und manche hierzulande erhobenen Forderungen nach „mehr Datenschutz“ müssen den Bürgern ärmerer Staaten als sehr fernliegend und typisch für eine Luxusgesellschaft erscheinen.

Um noch konkreter zu werden: Wir sollten uns zum Beispiel dazu bekennen, dass Frieden, gewaltfreie Streitlösung den Vorrang vor der individuellen Handlungsfreiheit haben muss, dass soziale Gerechtigkeit vor der Gewinnmaximierung Einzelner rangiert, dass Strafverfolgung und Gefahrenabwehr durch Polizei und Justiz grundsätzlich (also mit Ausnahmen) höherrangig sind als der Persönlichkeitsschutz durch das Steuer- oder Bankgeheimnis und dass das Sozialgeheimnis,

auf das sich Sozialarbeiter berufen, in manchen Situationen hinter dem Wohl eines Kindes zurückstehen muss. So wie es eine Sozialpflichtigkeit des Eigentums gibt, gibt es auch eine *soziale Einbindung des Persönlichkeitsrechts*. Dementsprechend muss der Aufwand, den der Staat und die Unternehmen betreiben, um persönliche Daten vor Ausspähung zu schützen, in einem angemessenen Verhältnis zu den Mitteln stehen, die für die Erfüllung anderer Pflichten verfügbar sind.

Wertungswidersprüche und -unsicherheiten

Weil über dergleichen Fragen zu wenig nachgedacht wird, begegnen wir in der öffentlichen Diskussion wie auch im Handeln von Staat und Wirtschaft irritierenden *Widersprüchen* und *Unsicherheiten* der Bewertung: Technische Innovationen wie die genaue Energieverbrauchsmessung, die einerseits im Zuge der Energiewende als große Fortschritte gefeiert werden, erscheinen andererseits als Teufelszeug, dessen Realisierung möglichst verboten oder zumindest streng eingeschränkt werden soll. So liest man derzeit in den Fachzeitschriften und den Tätigkeitsberichten der Datenschutzbeauftragten lange Artikel[16] über das Smart Metering, also die Technik der detaillierten, auf die einzelnen Geräte bezogenen Messung des Energieverbrauchs und der Nutzungszeiten: Diese Methode berge „ein hohes Ausforschungspotential hinsichtlich der Lebensgewohnheiten der Betroffenen".[17] Nützliche, bisher als bürgerfreundlicher Service angesehene Auskünfte der Verwaltung – wie die Melderegisterauskünfte an Private – werden plötzlich als „gesetzlicher Wahnsinn"[18] bezeichnet – als wäre der Zweck, bei Postsendungen Adressänderungen zu berücksichtigen, vollkommen abwegig.[19] Viele halten es für unerträglich, dass Wirtschaftsunternehmen potentiellen Kunden namentlich adressierte Werbung ins Haus schicken; der Nutzen der Werbung wird gering geschätzt. Selbst die Spendenwerbung für gemeinnützige Organisationen gilt manchen schon als rechtswidrige Handlung, wenn dabei Anschriften verwendet werden, die nicht ausdrücklich für diesen Zweck erlangt worden sind. Sogar die Werbung für Organspenden wird blockiert, weil angeblich schon eine gesetzliche Pflicht, sich zur eigenen Spendenbereitschaft zu äußern, „rechtlich, vor allem datenschutzrechtlich bedenklich" sei.[20] Die Freiheit der einen, auf die Frage nach der Spendenbereit-

16 Ein Beispiel: Hornung/Fuchs 2012 (mit zahlreichen weiteren Nachweisen ähnlicher Abhandlungen).
17 Entschließung der 80. Konferenz der Datenschutzbeauftragten, in: BfDI 2011, S. 57 f. Näheres dazu unten S. 59 f.
18 Bericht von Heribert Prantl über eine Äußerung des schleswig-holsteinischen Datenschutzbeauftragten Thilo Weichert, Süddeutsche Zeitung v. 7./8. 7. 2012.
19 Aus der Berichterstattung und Kommentierung der Medien sei nur auf Blechschmidt/Käppner 2012 und Esslinger 2012 verwiesen.
20 So der CDU-Bundestagsabgeordnete Jens Spahn laut Süddeutscher Zeitung vom 25.10.2011.

schaft nicht zu antworten, wird also höher bewertet als das Ziel, zur Hilfe für schwerstkranke Menschen beizutragen. Über derartige sozial-ethische Kontroversen muss diskutiert werden, und die Entscheidungen müssen in den Formen des Rechts getroffen werden, möglichst als Gesetz, hilfsweise als Richterrecht.

Eine Veränderung der Werteskala zeichnet sich auch in Sachen Urheberrecht ab. Wenn die bisher fest verankerten Rechte von Künstlern und Autoren, Verlagen und Produzenten zugunsten der Internet-Allgemeinheit beiseite gedrängt werden, geht es wirklich um Wichtiges: „Tausend fundamentale Fragen, die lang beantwortet schienen, stellen sich plötzlich neu".[21] Das erste Beispiel ist „das Konzept des Eigentums", das „durch illegale Downloads von Musik und Filmen partiell außer Kraft gesetzt worden" sei; das werfe die Frage auf, „ob sich das Recht noch durchsetzen lässt im virtuellen Raum, der jenseits nationalstaatlicher Grenzen organisiert ist". Wenn aber das Recht nicht mehr „vollstreckt" werden kann – „was bleibt dann, sehr zugespitzt gesagt, vom Staat überhaupt?"

Aber nochmals: Viele dieser Fragen lassen sich mit einiger Entschiedenheit beantworten. Nur sind die Antworten selten ein pauschales Entweder/Oder, sondern meist differenzierte Lösungen, in aller Regel Kompromisse.[22] Es gibt in keinem Bereich der menschlichen Gesellschaft unbegrenzte Freiheit für den Einzelnen, seine Wünsche durchzusetzen. Ein Teil der Internet-Freaks will das nicht wahrhaben und fordert eben diese Freiheit mit viel Pathos ein. Sie träumen von einer Welt, in der keine Regeln gelten (außer denen, die man sich selbst gegeben hat oder die man mit anderen vereinbart hat), daher auch niemand mit Sanktionen rechnen muss, wenn er sich nimmt, was er will. Aber auch das elektronische Netz gibt uns nicht die Chance, ein Leben zu führen, in dem die harten Realitäten der Offline-Welt ausgeblendet sind.

Zwar sind die Gedanken und Gefühle frei – aber wenn ich einen anderen Menschen beleidige oder bestehle, endet die Freiheit. Es kann dann keine Rolle spielen, ob die Grenzüberschreitung online oder offline geschieht. Lasse ich einen anderen erkennen, dass ich ihn missachte, so riskiere ich, von ihm belangt zu werden oder ihm Genugtuung verschaffen zu müssen. Wer einem anderen die Identität stiehlt oder sonstwie einen Schaden zufügt, muss damit rechnen, dass der ihn anzeigt und vor Gericht zieht. Nicht nur der Geschäftsverkehr in der Außenwelt, sondern eben auch die elektronisch vermittelten Rechtsgeschäfte können nicht „rechtsfrei" abgewickelt werden. Mag sein, dass es angemessener ist, manche Streitigkeiten im Schiedsverfahren zu bewältigen – aber auch das ist keine Besonderheit des Internethandels; auch im traditionellen Geschäftsleben wird manch ein Prozess nicht vor staatlichen Gerichten, sondern vor vereinbarten Schiedsgerichten ausgetragen. Mag sein auch, dass manche Streitfragen gar nicht nach rechtlichen Maßstäben

21 Wefing 2011 (auch die folgenden Zitate).
22 Sehr lesenswert dazu Passig/Lobo 2012.

entschieden werden, sondern dass es besser ist, sich mit einer moralischen Beurteilung zu begnügen – irgendwo jedoch beginnt der Bereich, in dem die moralische Verurteilung nicht mehr ausreicht, Frieden zwischen den Beteiligten herzustellen, und die Geschädigten nach harten rechtlichen Sanktionen verlangen.

Die Bestimmung der Akteure, Verantwortlichen und Nutznießer

Aufgabe des Rechts ist es auch, *Akteure* und damit *Verantwortliche* herauszuarbeiten (natürlich aufgrund politischer und medialer sozialethischer Diskussionen). Wenn nicht feststeht, welche natürliche oder juristische Person für eine Handlung oder einen Vorgang verantwortlich ist, kann kein Missstand ausgeräumt und kein Vergehen sanktioniert werden. In Teilen der Internet-Literatur scheint diese simple Erkenntnis noch nicht angekommen zu sein; sonst würden wir nicht immer wieder jene versponnenen Vorstellungen von der Wirkkraft des Netzes selbst lesen, die auf eine Verschmelzung von Menschen und Maschinen hinauslaufen und damit die Verantwortung für die Veränderung der Welt vernebeln. Der „Zukunftsforscher" Kevin Kelly wird mit dem Satz zitiert: „Je mehr wir diesen Megacomputer benutzen, desto mehr wird er die Verantwortung für unser Wissen übernehmen. Dann wird er unser Gedächtnis. Und dann unsere Identität". Eine Soziologin und Psychologin am berühmten MIT in Harvard namens Sherry Turkle soll erforscht haben, dass intensive Nutzer der diversen digitalen Geräte zu „einer Art Cyborg" werden, indem sie „mit der Technik in einer Weise eins" würden, „die noch vor wenigen Jahren auch für sie selbst unvorstellbar gewesen sei".[23] Ein neues Kunstwort, dessen Bedeutung man nur erahnen kann – ist das der Stoff, aus dem wir uns ein Urteil über soziale und geistige Entwicklungen bilden können?

Nein, für rechtliche und politische Zurechnungen ist diese Art von Computerwissenschaft unbrauchbar. Sie bedeutet nämlich den Verzicht auf eine Steuerung der gesellschaftlichen Prozesse. Die Frage nach der Verantwortung wird unbeantwortbar, eine Zurechnung von Handlungen zu Personen unmöglich; wer will schon einen „Megacomputer" oder einen „Cyborg" korrigieren oder zur Rechenschaft ziehen? Wenn aber menschliche Verantwortung entfällt, entfallen zugleich die Vorstellungen von Gut und Böse, Recht und Unrecht. Nichts stört dann mehr die Organisatoren bei ihren Geschäften! Solche Theorien sind also nicht nur für Juristen eine Zumutung. Sie hebeln auch politische Reaktionsmöglichkeiten aus, und man fragt sich, ob das ihren Urhebern wohl bewusst ist.

Für Freiheit und Rechtsschutz im Internet ist statt dessen die Frage bedeutsam, wer das Internet und seine einzelnen Elemente betreibt, wer also als Akteur ange-

23 Fischermann/Hamann 2012 S. 20.

sehen werden muss, an den sich rechtliche Anforderungen richten können. Die Staaten sind es nicht (ausgenommen sie betätigen sich als Zensoren und trennen nationale Netze von den internationalen Verbindungen!) , und es gibt überhaupt keinen Alleinbetreiber oder Alleinverantwortlichen für das weltweite Netz, sondern verschiedene Netzbetreiber und zahllose Anbieter von Diensten aller Art, riesige, große und kleine Unternehmen, Einzelpersonen und Vereinigungen, seriöse und unseriöse, altruistische und raffgierige.

Entstanden ist das Internet bekanntlich aus Datenübertragungsnetzen, die das US-amerikanische Verteidigungsministerium für Forschungszwecke eingerichtet hat.[24] Dabei sollte die Anfälligkeit der bis dahin bestehenden Verbindungen durch eine dezentrale Anordnung beseitigt werden; bei Störungen der einen Leitung sollte automatisch auf eine andere ausgewichen werden. Dieses Prinzip hat sich sofort bewährt und wurde für zivile Zwecke übernommen. Computerfirmen und Informationsversorger in aller Welt sahen die Chance, Transportleistungen für Datenpakete zu verkaufen – und das Ergebnis ist die globale Vernetzung aller, die es sich leisten können, vor allem der Unternehmen und Behörden, national wie international. In wenigen Jahren entstand ein dichtes Netz von Leitungen und Computern („Servern"), die den Verkehr auf den Datenleitungen steuern und gesuchte Inhalte aus den Datenmassen heraussuchen und auf die einzelnen Computer befördern.

Die Frage, wer für die im Netz gespeicherten und übermittelten Inhalte verantwortlich ist, wird damit immer schwieriger zu beantworten. Manche Beteiligten sind bloß Nutznießer, „Mitläufer"; inwieweit sie für Fehler und Rechtsverstöße verantwortlich gemacht werden können, ist zweifelhaft; andere arbeiten hochprofitabel und stehen im Zentrum des öffentlichen Interesses und der Kritik.

Ein möglicher und sinnvoller Anknüpfungspunkt für rechtliche Zurechnung ergibt sich aus der Gewinnträchtigkeit der jeweiligen Aktivtäten. Ausgleichende Gerechtigkeit verlangt, dass derjenige, der aus einer Einrichtung Vorteile zieht, auch die Nachteile tragen muss, die dadurch regelmäßig entstehen, also z.B. für Fehler haften muss. Bisher wird das Internet teilweise aus Netzanschlussentgelten finanziert, die an die Betreiber der Telekommunikationsnetze und der vermittelnden Server gezahlt werden, und in geringem Umfang auch aus zusätzlichen Gebühren, die für Sonderdienste zu entrichten sind. Die Unternehmen, die das Suchen und Befördern von Informationen anbieten, bestreiten den größten Teil ihrer Kosten aus Entgelten für die Werbeeinblendungen, die sie auf ihren Seiten platzieren, und aus der Vermarktung personenbezogener Daten über die Nutzer zum Zwecke der immer raffinierter werdenden Werbung. Das Profitstreben der Unternehmen ist zwar noch kein ausreichendes Kriterium für die Zurechnung von Rechtsverletzungen, aber wenn sie mit der Herrschaft über die Daten und der Möglichkeit zur

24 Eine Darstellung der Entstehungsgeschichte findet sich u.a. bei Werle 2000, s. 142 ff.

Vermeidung von Beeinträchtigungen verbunden ist, spricht viel für eine rechtliche Verantwortlichkeit der Netzbetreiber oder zumindest der Diensteanbieter. Das geltende Telemediengesetz bestimmt, dass Diensteanbieter für die Speicherung, Durchleitung oder Übermittlung fremder Informationen nur ausnahmsweise verantwortlich sind,[25] aber diese Regelung ist durchaus umstritten und könnte geändert werden. Es ist eine wichtige Aufgabe der Netzpolitik, in dieser Frage mehr Klarheit zu schaffen.[26]

Die Staaten haben ebenfalls Interessen in Bezug auf das Netz. Sie wollen an den Vorteilen des Netzes teilhaben, also selbst als Nutzer mit im Spiel sein. Andererseits müssen sie gegenüber anderen Nutzern und gegenüber den Betreibern ihre Rechtsordnung zur Geltung bringen, sofern die Nutzung in Formen geschieht, die nach der nationalen oder völkerrechtlichen Ordnung rechtswidrig sind. An der Gesamtleistung „Internet" sind sie bisher nur marginal beteiligt, etwa durch Bereitstellen von Leitungen (in Deutschland überwiegend eine Aufgabe von Staat und Kommunen, die aber von Konzessionsnehmern wie der Deutschen Telekom ausgeführt wird). Aber das kann sich ändern.[27]

Die große „Gemeinde" der Internetnutzer kann sich nur mittelbar, über die Regierungen und Parlamente der Staaten und einige supra- oder internationale Organisationen äußern. Eine Grundvoraussetzung des Internetbetriebs, die Zuordnung der Anschlüsse unter einer eindeutigen Identifizierung, also einer Nummernfolge, die niemandem sonst zugewiesen ist, wird auf der obersten Ebene, bei den übergreifenden „Domains", von einer privaten Organisation gewährleistet. Das ist eine merkwürdige Geschichte: Das amerikanische Handelsministerium hat diese Aufgabe Mitte der 1990er Jahre an eine halbamtliche Organisation namens *Internet Assigned Numbers Authority (IANA)* übertragen, von der es heißt, ihr einziger Mitarbeiter sei der Internet-Pionier *Jonathan Postel* gewesen. 1998 wurde diese Organisation in eine andere integriert, die sich *Internet Corporation for Assigned Names and Numbers (ICANN)* nennt.[28] Bei ICANN handelt es sich um eine Non-

25 Vgl. §§ 8-10 TMG.

26 Dazu Spindler 2012, S. 60 ff. S. a. unten S. 35 mit Fn. 59. Über die Verantwortlichkeit der Internetprovider oder „Intermediären" für Urheberrechtsverletzungen und ihre entsprechenden Pflichten zur Filterung von Inhalten wird vor nationalen und europäischen Gerichten inzwischen heftig gestritten. Der EuGH hat die geltenden EU-Richtlinien so ausgelegt, dass Anbieter von Internetzugangsdiensten nicht dazu verpflichtet werden dürfen, ein umfassendes und „perfektes" System der Filterung aller seine Dienste durchlaufenden elektronischen Kommunikationen einzurichten; vgl. Urteil v. 24.11.2011, JZ 2012, 308 (Scarlet ./. SABAM) m. zust. Anm. und weiteren Hinweisen von Spindler S. 311. Die Diskussion ist damit aber noch lange nicht beendet (so auch Spindler, JZ 2012, 312 f.).

27 Interessante, historisch fundierte Überlegungen dazu bei Passig/Lobo 2012, S. 177 ff.

28 Eisel 2011, S. 65; dort auch Details zur Verwaltung der deutschen Top Level Domain „de": Die deutschen Internet Service-Provider vergaben die Domainverwaltung nach einer Ausschreibung an das Rechenzentrum der Universität Karlsruhe. Später gründeten die deutschen Service-Provider eine Genossenschaft zur Domainverwaltung, die DENIC mit Sitz in Frankfurt am Main. S.a. Ahlert, in: Holznagel/ Grünwald/Hanßmann 2001, S. 44 ff.

Profit-Organisation, genauer eine privatrechtliche Stiftung nach US-amerikanischem Recht mit Sitz in Marina del Rey in Kalifornien. Die Regierungen sind im Governmental Advisory Committee vertreten, aber im Wesentlichen handelt es sich um eine Form von Selbstregulierung der interessierten Kreise, Unternehmen und Verbände – angesichts der Aufgabe der Organisation vielleicht eine angemessene Form. Wie diese wichtige Organisation tatsächlich funktioniert, ist für den Außenstehenden freilich schwer zu erkennen. Klar ist nur, dass auch hier Macht ausgeübt wird. Die angebliche Hierarchiefreiheit der Internet-Organisation ist eine Legende.

Ob die Regierungen sich dauerhaft zurückhalten, ist ungewiss.[29] Soweit bei der Nummernvergabe wiederholt oder gar systematisch ungerecht – gleichheitswidrig und diskriminierend oder protektionistisch – vorgegangen werden sollte, werden sie sich mit Sicherheit einmischen; denn schon um seiner eigenen Legitimation willen kann kein Staat sich vor der Verantwortung drücken, wenn die privat-gesellschaftliche Organisation ihre Aufgabe verfehlt. Arme und Reiche, eigene und fremde Staatsangehörige müssen gleich behandelt werden, das lässt sich grenzüberschreitend mit Verbindlichkeit nur durch Übereinkünfte der Staaten garantieren. Auch die internationale Gerichtsbarkeit wird sich eines nicht sehr fernen Tages mit derartigen Streitfragen beschäftigen müssen.

Die offenen Flanken des Rechtsschutzes – und wie sie zu schließen sind

Ubiquität und *Internationalität* kennzeichnen den heutigen Stand der Datenverarbeitung: Die Computer sind überall, in miniaturisierter Form sogar in allen möglichen Gegenständen und als Herzschrittmacher oder Messgeräte im menschlichen Körper. Unzählige Computer sind über alle nationalen Grenzen und Staatenverbünde hinweg miteinander verbunden, und gewaltige Datenmengen werden irgendwo in der weiten Welt, wo gerade Platz ist, in „clouds“ gespeichert, und diese „Wolken“ kennen erst recht keine nationalen Grenzen, sondern „regnen“ ihren Inhalt mal hier, mal dort ab.

Für den Rechtsschutz hat diese Entwicklung fast unlösbare Probleme verursacht. Die Durchsetzung von Individualrechten erscheint so gut wie aussichtslos, wenn die Daten, um die es geht, nicht mehr nur einmal in einer bestimmten Datei gespeichert sind, sondern an eine Vielzahl von Adressaten übermittelt werden, und wenn jeden Augenblick neue Daten erzeugt und verarbeitet werden. Die Betroffe-

29 Es gibt bereits Bestrebungen, Aufgaben der ICANN auf die Internationale Fernmeldeunion ITU zu übertragen, also auf eine internationale Organisation, die zur UNO gehört und damit jedenfalls mittelbar dem Einfluss der Regierungen unterliegt, vgl. Küchemann 2012. Ob diese Organisationsform besser wäre, lässt sich schwer sagen.

nen und ihre Rechtsanwälte, aber auch die Richter und Staatsanwälte müssen hinter den Akteuren herlaufen und holen sie selten ein. Der Einzelne, der sein Recht sucht, ist regelmäßig schon mit der Aufgabe überfordert, die Verantwortlichen herauszufinden, geschweige denn ein Unternehmen wie Facebook oder Google zu verklagen. Auch strafrechtlich werden Datenschutzverstöße in Deutschland bisher kaum verfolgt.[30] Bei den internationalen Internetfirmen kommt zu dem normalen Prozessrisiko hinzu, dass sie nach fremdem Recht agieren und in ihren Geschäftsbedingungen einseitig bestimmen, welche Rechte und Pflichten die Vertragspartner haben – ein Machtübergewicht der Betreiber, gegen das Einzelne nur schwer ankommen können.

Gleichwohl ist es nicht vollkommen aussichtslos, individuelle Rechte auch gegen die mächtigen Unternehmen durchzusetzen. Sind andere Unternehmen betroffen, so pflegen sie ihre Interessen trotz der dargestellten Schwierigkeiten mit Nachdruck zu verfolgen; ihnen stehen hochspezialisierte Anwaltskanzleien zur Seite. Aber auch „der kleine Mann" kann manches erreichen, wenn er hartnäckig genug ist. Der Wiener Jurastudent Max Schrems hat den Großkonzern Facebook in Verlegenheit gebracht und erste organisatorische Änderungen bei ihm provoziert, indem er schlicht Auskunft über die von ihm gespeicherten Daten verlangte: Facebook lieferte ihm eine unerwartet umfangreiche Auskunft, darunter viele Daten, die längst hätten gelöscht sein müssen und teilweise auch als gelöscht bezeichnet waren. Schrems zeigte Facebook bei der zuständigen Datenschutzaufsichtsbehörde, dem irischen Data Protection Commissioner an, u.a. wegen irreführender Geschäftsbedingungen und anderer Verstöße gegen europäisches Recht, und setzte damit Ermittlungen in Gang, die von dem Konzern offenbar mit größtem Unbehagen zur Kenntnis genommen wurden.[31] Die Sache ist für die Kritiker noch lange nicht gewonnen, aber dass Facebook diese Nadelstiche ernst nimmt, zeigt sich auch darin, dass sein Europa-Bevollmächtigter Richard Allan versuchte, Schrems von einer Klage abzubringen.[32] Übrigens sind inzwischen viele andere Facebook-Nutzer dem Vorbild des „aufmüpfigen" Juristen gefolgt und setzen Facebook mit ihren Beschwerden zu.

Leichter wäre es für die betroffenen „Normalnutzer", wenn es ein Verbandsklagerecht von Organisationen gäbe, die die verschiedenen Klagen und Beschwerden bündeln könnten. So wird vorgeschlagen, nach dem Vorbild des Umweltschutzes speziellen Verbänden von Datenschützern ein Klagerecht einzuräu-

30 Sieber 2012, S. 29 mit Hinweis auf die amtliche Kriminalstatistik.

31 Prummer 2012. Unter dem Titel „Europe versus Facebook" betreibt Schrems eine Webseite mit zahlreichen Nachweisen zur Medienberichterstattung (www.europe-v-facebook.org). Der Bericht der irischen Behörde Data Protection Commissioner: Facebook Ireland Ltd. – Report of the Re-Audit, 21 September 2012) ist zugänglich unter www.dataprotection.ie . Danach muss Facebook nunmehr z.B. die Gesichtserkennung abschalten.

32 Prummer 2012.

men.[33] Die Verbandsklage ist jetzt auch in dem Entwurf der Europäischen Datenschutz-Grundverordnung vorgesehen.[34] Damit wird an die amerikanische Methode angeknüpft, in „Sammelklagen" („class actions") den Rechtsschutz gegen solche Verstöße zu bündeln, die für sich genommen einen Prozess nicht lohnen. Diese Konstruktion würde einen neuen Markt für Juristen eröffnen – vermutlich mit ähnlichen Folgen wie derzeit bei Urheberrechtsstreitigkeiten, dass nämlich Spezialisten für „Abmahnungen" damit gute Geschäfte machen. Die Rechtsentwicklung aber könnte dadurch vorangetrieben werden; denn auf diese Weise würden aus vielen kleinen Fällen neue Regeln entwickelt - Richterrecht, das konkreter und sachnäher sein kann als die allgemein gehaltenen gesetzlichen Vorschriften.

Ein anderer Vorschlag zielt darauf ab, „grenzüberschreitende onlinespezifische Schiedsverfahren" einzurichten.[35] Auch damit könnte einiges bewirkt werden – freilich wohl in erster Linie zwischen hinreichend großen, organisationsstarken Unternehmen und Verbänden.[36] Microsoft, Google und Facebook mögen auf diesem Wege ihre Rechtsstreitigkeiten bewältigen und neue verbindliche Regeln produzieren, aber es dürfte schwer sein, die Betroffenen in diese Schiedsverfahren einzubeziehen.

Die Grenzen der nationalen Rechtsordnung[37] können jedenfalls in der Europäischen Union überwunden werden, indem gemeinsames Recht geschaffen wird. Das wird gegenwärtig versucht: Es wird intensiv über den erwähnten Entwurf einer Datenschutz-Grundverordnung beraten. Die damit intendierte umfassende und intensive Regelung des Datenschutzes stößt allerdings auf Bedenken: Diejenigen EU-Mitgliedstaaten, die wie die Bundesrepublik ein hohes Datenschutzniveau haben,[38] wollen darauf nicht verzichten; ein Richter des Bundesverfassungsgerichts sieht sogar die weltweit beachtete Rechtsprechung dieses Gerichts und die Geltung unserer Grundrechte in der Gefahr, einer Nivellierung auf europäisches Mittelmaß zum Opfer zu fallen.[39] Andererseits wird es wohl kaum eine europäische Rechtsharmonisierung geben, wenn für alle Mitgliedstaaten der höchste denkbare Standard gefordert wird.

Der Europarat hat vor einigen Jahren eine „Cybercrime-Konvention" beschlossen,[40] die eine Vereinheitlichung der in Betracht kommenden Straftatbestände verlangt, aber keine spezifischen Regelungen zur Gerichtsbarkeit enthält. Es gibt auch

33 S. etwa Spindler 2012, S. 130 f. m.w.N.
34 Vgl. Europäische Kommission 2012, Art. 75 Abs. 2 und Art. 76 Abs. 1 des Entwurfs.
35 Spindler 2012, S. 113 f. und These 11, S. 134.
36 S. aber auch den Vorschlag von Ladeur 2012, unabhängige „Cyber-Courts" einzurichten; dazu noch unten S. 124 f.
37 Dazu grundsätzlich und ausführlich Determann 1999. S. a. Franda 2001.
38 Schaar 2007, S. 26 mit Hinweisen auf „internationale Hitlisten".
39 Masing 2012 a.
40 Vgl. Sieber 2012, S. 41 und 75.

Initiativen der EU über die geplante Datenschutz-Grundverordnung hinaus, und es gibt Forderungen nach einer UN-Konvention.[41]

Selbst internationale Rechtshilfe läuft ins Leere, wenn die einschlägigen Rechtsvorschriften die Anwendung einer Rechtsordnung gebieten, die dem Betroffenen im konkreten Fall keine ausreichenden Rechte zuweist. Das geschieht häufig, wenn Europäer versuchen, Verstöße gegen ihre Vorstellungen von Datenschutz in angelsächsischen Ländern zu verfolgen. So „ordnet das Recht der Vereinigten Staaten von Amerika den Datenschutz über ein Flickwerk von Regeln, die große Bereiche frei von jeder formellen Regulierung lassen".[42] Berichtet wird von einem deutschen Richter, „der Zugriff auf Facebookdaten suchte, dann auf die Facebook-Niederlassung in Irland verwiesen wurde und diese schließlich erklärte, dass die Daten leider auf Servern in den USA lägen".[43] Dieser Fall macht übrigens deutlich, dass es nicht sachgerecht ist, an den Ort der Datenspeicherung und damit den Sitz des Anbieters anzuknüpfen; die Rechtsverfolgung muss vielmehr dort möglich sein, wo der Nutzer seinen Sitz hat – die Experten sprechen vom „Marktortprinzip".[44]

Wenn die Europäische Datenschutz-Grundverordnung verbindlich wird, ergibt sich innerhalb der Union eine weitgehend einheitliche Rechtslage. Aber jeder, der einmal mit der Anwendung unbestimmter Rechtsbegriffe zu tun hatte, weiß um die Schwierigkeiten, solche Normen einheitlich anzuwenden. Enthält eine Vorschrift Begriffe wie „öffentliches Interesse" oder „Wesensgehalt des Rechts auf den Schutz personenbezogener Daten", so sind ganz unterschiedliche Interpretationen und folglich eine divergierende Anwendung der Norm unvermeidlich. Die zitierten und ähnlich weite Formulierungen stehen in der EU-Grundverordnung an mehreren zentralen Stellen.[45] Immer wieder bedingen Datenschutzvorschriften des nationalen und supranationalen Rechts eine Abwägung zwischen verschiedenen Grundrechten oder Interessen, ohne dass dazu Richtlinien gegeben würden – auch dies eine Quelle ständiger Meinungsverschiedenheiten.

Deren Lösung erfordert Zuständigkeitsregeln, die einer der beteiligten Instanzen die verbindliche Entscheidung zuweist. Die EU-Verordnung versucht dies zunächst, indem sie die nationalen Aufsichtsbehörden zur gegenseitigen Amtshilfe verpflichtet und ihnen gemeinsame Maßnahmen gestattet und vor allem ein geregeltes „Kohärenzverfahren" einführt.[46] Zusätzlich wird ein unabhängiger Europäischer Datenschutzausschuss eingerichtet, der durch Beratung der Kommission

41 So etwa Dix, in: DJT 2012, S. 73 These 19.
42 Paul M. Schwartz, in: DJT 2012, S. 75 These 2.
43 Masing 2012 b, S. 2310 m.w.N.
44 Osthaus, in: DJT 2012, S. 75 These 15; Spindler ebd. S. 68 These 14.
45 Vgl. Europäische Kommission 2012, Art. 6 Abs. 3 (betrifft die Rechtmäßigkeit der Datenverarbeitung) und Art. 17 Abs. 3 Buchstabe d (betrifft Ausnahmen von der Pflicht zur Löschung von Daten). Auf das „öffentliche Interesse" stellen noch weitere Normen der EG-Grundverordnung ab.
46 Art. 55-63 des Entwurfs.

und Stellungnahmen zu Beschlussentwürfen im Kohärenzverfahren die einheitliche Anwendung der Verordnung „sicherstellen“ soll.[47] Bei wesentlichen Streitfragen wird ihm dies aber wohl kaum gelingen. Zwar kann mit den bezeichneten Vorkehrungen gewiss ein hohes Maß an Einheitlichkeit erreicht werden, aber eben keine verbindliche Letztentscheidung.[48] In einigen besonderen Fällen kann die Kommission „Durchführungsrechtsakte“ erlassen,[49] aber im Prinzip behalten die nationalen Aufsichtsbehörden die Verantwortung für ihre Entscheidungen, und die Betroffenen müssen sich um Rechtsschutz vor den nationalen Gerichten bemühen.[50]

Einen weiteren Ansatz der Vereinheitlichung bildet jedoch die vorgesehene Befugnis der Kommission, „delegierte Rechtsakte“ zu erlassen, die der Konkretisierung der unbestimmten Formulierungen dienen sollen.[51] Auch darüber wird es noch viel Streit geben; denn die Kommission muss dann all die konkreten Abwägungen nachholen, die vor dem Entwurf der Verordnung versäumt worden sind.

Aber nochmals: Der Versuch einer Vereinheitlichung ist richtig, die einzelnen Instrumente dafür müssen diskutiert werden, und auf der Ebene der Vereinten Nationen sind weitere Schritte nötig. Denn es ist ja Konsens, dass die Menschen auf der ganzen Welt vor den Risiken der Informationstechnik geschützt werden müssen. Ohne verpflichtendes Recht ist dies unmöglich.

47 Art. 64-72, Zitat: Art. 66 Abs. 1 Satz 1.
48 Daher fordert Dix (in: DJT 2012, S. 73 These 20) das Letztentscheidungsrecht des Europäischen Datenschutzausschusses.
49 Art. 62.
50 Art. 74 und 75.
51 Vgl. Art. 86 mit der langen Liste der Einzelermächtigungen! Weiteres s. unten S. 142 f.

Erster Teil: Die Rechte des Individuums

Freiheit und Freiheiten

Die einschlägigen Grundrechte

Die Rechtslage des Individuums in der „Informationsgesellschaft" wird heute regelmäßig zunächst unter dem Aspekt des Datenschutzes und seiner Bedrohung erörtert. Es ist aber angebracht, zuerst *alle* in Frage kommenden Rechte des Einzelnen zu behandeln; von ihnen aus können und müssen dann die Risiken und Bedrohungen angesprochen werden, und von ihnen aus sind auch Grenzen der Freiheit zu bestimmen. In diesem Sinne also als erste Feststellung: Der Einzelne hat *subjektive Rechte*, die ihm kraft Verfassung oder sogar kraft internationalen Rechts zustehen; diese Rechte gelten auch, wenn wir uns ins Internet begeben und dort an Informations- und Meinungsaustausch teilnehmen.

Im Prinzip gilt für die Kommunikationsvorgänge im Netz, was auch für den Austausch außerhalb des Netzes gilt: Die in Art. 5 Abs. 1 GG gewährleisteten Grundrechte der Meinungs-, Presse- und Rundfunkfreiheit sind hier wie dort die Bastionen der politischen Freiheit, aber auch die zensurfreien (Art. 5 Abs. 1 Satz 3 GG!) Tore für Spiel und Unterhaltung. Die Meinungsfreiheit umfasst nach der Rechtsprechung des Bundesverfassungsgerichts nicht nur „Werturteile", sondern auch die Freiheit, wahre (!) Tatsachenbehauptungen zu verbreiten.[52] Dem Internetnutzer, der sich nur informieren will, steht das ebenfalls in Art. 5 Abs. 1 GG garantierte Recht zur Seite, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten". Die Pressefreiheit und „die Freiheit der Berichterstattung durch Rundfunk und Film" werden weit ausgelegt und von manchen Autoren schlicht als „Medienfreiheit" bezeichnet. Dagegen ist nichts einzuwenden. Soweit allerdings eine „Freiheit der Internetdienste" angenommen wird,[53] ist dies zumindest missverständlich, denn „die Dienste" sind keine Akteure wie die Zeitungsverlage und Fernsehunternehmen; hinter ihnen stehen zunächst einmal natürliche oder juristische Personen, die ihre unternehmerische Freiheit nutzen (und deren Schranken beachten müssen, die sich von denen der Medienunternehmen unterscheiden können). Überzeugender ist es, für allgemeine Aussagen die Grundform der einschlägigen Freiheitsrechte zugrunde zu legen, also auf das Recht zur unge-

52 Vgl. u.a. BVerfGE 54, 208 (219); 61, 1 (7 f.); 85, 1 (14 f.);
53 Spindler 2012, S. 28 mit Nachweisen in Fn. 127. Dagegen u.a. Dix, in: DJT 2012, S. 72 These 13.

hinderten Äußerung und Verbreitung von Meinungen und wahren Tatsachen abzustellen. Diese Rechte können als „Äußerungs- und Kommunikationsfreiheit“ zusammengefasst werden.

Freiheit im Netz

Das Internet kann aber ebenso wenig ein „rechtsfreier Raum“ sein wie die übrige Welt. Die Rechte des Art. 5 Abs. 1 GG „finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre“ (Art. 5 Abs. 2 GG). „Allgemeine Gesetze“ sind solche, die nicht gegen die Meinungsfreiheit als solche gerichtet sind, sondern ohne Rücksicht auf die Meinungsäußerung andere Rechtsgüter schützen sollen. Zu den „allgemeinen Gesetzen“ zählen u.a. die Bestimmungen des Zivilrechts zum Schutze materieller und immaterieller Güter anderer und das Recht des „geistigen Eigentums“. Meinungsfreiheit soll dazu beitragen, dass geistiger Austausch und Auseinandersetzung möglich sind; das Grundgesetz unterscheidet auch nicht zwischen „wertvollen“ und „wertlosen“ oder „richtigen“ und „falschen“ Meinungen. Aber Meinungsfreiheit rechtfertigt es nicht, andere zu belästigen, zu beschimpfen oder durch unwahre Behauptungen in ihrer beruflichen oder gewerblichen Betätigung zu schädigen. Die Meinungsfreiheit der einen kollidiert oft mit dem Anspruch der anderen auf Privatsphäre und Persönlichkeitsschutz; in zahllosen Fällen war eine schwierige Abwägung nötig – was zu vielen Gerichtsentscheidungen über heikle Einzelfälle geführt hat. Die bekanntesten sind die Urteile höchster Gerichte (bis hin zum Europäischen Gerichtshof für Menschenrechte) in Sachen Caroline von Monaco gegen die Boulevardpresse). Schon bevor der Gedanke des Datenschutzes aufkam, ist auf diese Weise ein liberales System des „Äußerungsrechts“ entstanden.[54]

Ohne solche Schranken wäre das Miteinander der Menschen oft unerträglich. Gerichte und Rechtwissenschaft haben die Schranken ihrerseits so ausgestaltet, dass sie das Grundrecht nicht in seinem Kern beschädigen. Berühmt ist die Definition der „allgemeinen Gesetze“ durch das Bundesverfassungsgericht: Das sind solche, „die sich nicht gegen die Äußerung einer Meinung als solche richten, die vielmehr dem Schutz eines schlechthin, ohne Rücksicht auf eine bestimmte Meinung, zu schützenden Rechtsgutes dienen“. Die „allgemeinen Gesetze“ müssen „im

54 S. unten S. 51 ff..

Lichte der besonderen Bedeutung des Grundrechts der freien Meinungsäußerung für den freiheitlichen demokratischen Staat ausgelegt werden".[55]

Eines besonderen Grundrechts für die Kommunikation bedarf es daher nicht, und wenn dieses als schrankenlos verstanden würde, wäre es mit dem Grundgesetz nicht vereinbar. Die Forderung nach „Freiheit im Netz" kann allenfalls als ein Argument dazu dienen, die Handlungs- und Äußerungsfreiheit des Individuums (und die unternehmerischen Grundrechte der Betreiber) nicht zu eng zu begrenzen. Schwer vorstellbar, aber immerhin möglich ist es freilich, dass sich eines Tages die Meinung durchsetzt, man dürfe im Internet Dinge sagen, die unter Anwesenden nicht geduldet werden – das wäre dann ein Beispiel für eine neue Freiheit *im Netz*, aber keines für die Freiheit *des Netzes* vom Recht.

Als „allgemeines Gesetz", das die Freiheitsrechte des Art. 5 Abs. 1 GG einschränkt, ist im Jahre 1977 das Bundesdatenschutzgesetz (BDSG) mit seinen Regelungen über den richtigen Umgang mit Informationen hinzugekommen. Es will die Meinungs- und Medienfreiheit nicht einschränken, aber es kann faktisch zu erheblichen Einschränkungen oder zumindest Erschwerungen führen. Wer personenbezogene Daten Dritter in das Netz einstellt – und das geschieht in den sozialen Netzwerken, aber auch in anderen Teilen des Internet ständig –, speichert und übermittelt diese Daten, was nach der Grundvorschrift des BDSG (§ 4 Abs. 1) nur zulässig ist, „soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat". Die Einwilligung fehlt in zahllosen Fällen, und nach einer passenden Rechtsvorschrift wird man vergeblich suchen: Es gibt keine ausdrückliche Norm, die eine solche Erlaubnis oder Anordnung enthält. (Und falls jemand meinen sollte, die Erlaubnis ergebe sich aus dem Äußerungs- und Kommunikationsgrundrecht, so läge daran ein Zirkelschluss; denn dieses Grundrecht ist eben keine Erlaubnisnorm, sondern der Maßstab, an dem das Datenschutzgesetz als „allgemeines Gesetz" im Sinne von Art. 5 Abs. 2 GG gemessen werden muss). Man könnte allenfalls erwägen, dass Art. 5 Abs. 1 GG es erforderlich mache, einen Erlaubnistatbestand für Veröffentlichungen im Internet zu beschließen. Denn die gegenwärtige Rechtslage ist geradezu peinlich: Während es jedem frei steht, offline (wahre) Behauptungen über andere zu verbreiten, muss derselbe Vorgang, wenn das Internet als Transportmedium genutzt wird, vor dem BDSG gerechtfertigt werden, und unter Umständen kann eine Datenschutzauf-

55 BVerfGE 7, 198 (209); 62, 230 (244); 71, 162 (175); 85, 1 (16 f.). Das erstgenannte Urteil erging in einem Aufsehen erregenden Fall: Der Leiter der Hamburger Staatlichen Pressestelle, Erich Lüth, hatte zum Boykott eines Filmes von Veit Harlan, dem Regisseur von „Jud Süß" und anderen Propagandafilmen der Nazis, aufgerufen; nach bisherigem Recht lag darin ein Verstoß gegen das „allgemeine Gesetz", das die Schädigung Dritter verbietet (§ 826 BGB). Das BVerfG legte Art. 5 Abs. 2 GG so aus, dass der Meinungsfreiheit im konkreten Fall der Vorrang vor dem Zivilrecht zukam.

sichtsbehörde ihn verbieten oder reglementieren; hinzu kommen Unterrichtungs- und Auskunftspflichten gegenüber den Betroffenen.

Um dergleichen „bürokratische" Hindernisse auszuräumen, ist der Journalismus von vornherein vom Datenschutz ausgenommen worden. Das BDSG schreibt den Ländern vor, in ihren Gesetzen dafür zu sorgen, dass die „Unternehmen und Hilfsunternehmen der Presse" bei journalistischer Betätigung vom Datenschutz weitgehend freigestellt sind: In diesem Bereich gelten nur einige wenige Vorschriften (über das „Datengeheimnis" und den technischen und organisatorischen Datenschutz) (§ 41 BDSG). Wer aber ohne „journalistisch-redaktionelle oder literarische Zwecke" Informationen sammelt und verwendet, soll sich dafür nach den Regeln des Datenschutzrechts rechtfertigen müssen? Um auch das zu verhindern, halten manche es für angebracht, neben dem „Medienprivileg" auch ein „Laienprivileg" zu behaupten, das die Veröffentlichung von Tatsachen und Meinungen durch Nicht-Journalisten gegen Forderungen des Datenschutzes abschirmt.[56] Dafür spricht, dass die Äußerungsfreiheit nicht auf die Medien beschränkt ist; sie steht jedem und jeder zu. Ob aber wirklich die rechtliche Gleichstellung von Journalismus und Laienkommunikation geboten ist, kann mit gutem Grund bezweifelt werden.

Die *passive* Freiheit im Netz, das Suchen nach Informationen und Unterhaltung, ist selbstverständlich ebenfalls erlaubt und muss erlaubt bleiben, und solange dadurch niemandes Rechte berührt werden, darf und sollte das Surfen im Netz unbeobachtet geschehen. Wer nur lesen oder hören will, braucht seinen Namen nicht anzugeben. Die Diensteanbieter müssen diesen Wunsch nach Anonymität beachten.[57] In diesem Zusammenhang fordert der Berliner Datenschutzbeauftragte Alexander Dix, ein „Mediennutzungsgeheimnis" ausdrücklich festzulegen[58]– aber nur für den passiven Nutzer. Mit Recht betont Dix die Verantwortlichkeit der aktiven Nutzer: „Wer … aktiv Informationen im Netz veröffentlicht, sollte dies in pseudonymer Form (oder unter Klarnamen) tun müssen. Nur so können Datenschutz- und andere Rechtsverstöße verfolgt werden".[59]

Übrigens darf auch der Staat durch seine Behörden die „Freiheit" des Internets nutzen und sich mit allgemein zugänglichen Informationen bedienen. Das hat das

56 Christoph Fiedler auf der Datenschutz-Konferenz des BMI und des Humboldt-Instituts für Internet und Gesellschaft, Berlin 17./18.10.2012 (unveröff.).

57 Vgl. Telemediengesetz (TMG) § 13 Abs. 6: „Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren".

58 DJT 2012, S. 71 These 8.

59 DJT 2012, S. 71 These 8. Diensteanbieter sind nach § 7 Abs. 1 TMG „für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich", aber nach Abs. 2 dieser Vorschrift bei der Durchleitung oder Zwischenspeicherung fremder Informationen „nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen". Dazu auch §§ 8-10 TMG.

Bundesverfassungsgericht in dem Urteil über die Online-Durchsuchung privater Computer ausgesprochen, war also insofern weniger behördenkritisch.[60] Nicht erlaubt ist es danach aber, dass eine staatliche Stelle „sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt" und dabei „ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Informationen zu erheben, die sie sonst nicht erhalten würde".[61] Der behördliche Internetsurfer wird hier mit einem verdeckten Ermittler gleichgestellt, der sich das Vertrauen von Kriminellen erschlichen hat – ein Vergleich, der mit der üblichen Anonymität der Internetnutzung nicht ganz vereinbar ist. Das Gericht schickt selbst die Bemerkung nach, dass im Internet normalerweise kein Vertrauen aufgebaut wird, also auch nicht enttäuscht werden kann; man kennt ja die Identität der Partner meist nicht und kann sie nicht überprüfen.

Informationsfreiheit versus Geheimsphären

Die Computer-Ethik des CCC sagt: „Private Daten schützen, öffentliche Daten nützen!" Ein eingängiges Motto, nach dem sich der Gesetzgeber schon in der Vergangenheit gerichtet hat: Personenbezogene Daten werden geschützt, Daten der öffentlichen Verwaltung stehen – im Prinzip – jedem zur Verfügung. Leider sieht die Wirklichkeit etwas anders aus als dass die Zweiteilung zweifelsfrei umgesetzt werden könnte. Weder ist eindeutig, was „privat" ist, noch gehören alle vermeintlich „öffentlichen" Daten wirklich der Allgemeinheit. Es lohnt, sich mit diesem Thema näher zu beschäftigen.

Die Freiheit, sich aus allgemein zugänglichen Quellen ungehindert zu informieren, steht im Grundgesetz gleich nach der Meinungsfreiheit (Art. 5 Abs. 1 S. 1 GG). Sie folgt auch aus anderen Freiheitsrechten, z. B. der Berufsfreiheit: Wenn ich einen Beruf richtig ausüben will, muss ich zahllose Kontakte aufbauen und pflegen und deshalb auch Informationen über andere Menschen sammeln und verwerten. Die Informationstechnik hat gewaltige Chancen eröffnet, diese Freiheit tatsächlich zu nutzen, und die Gesetze fördern ihre Wahrnehmung. Denn es gelten

60 BVerfGE 120, 274 Leitsatz 6 und S. 344 ff. Eine Ausnahme macht das Gericht schon an dieser Stelle, indem es hinzufügt, dass „ein Eingriff in das Recht auf informationelle Selbstbestimmung" gegeben sein könne, wenn Informationen aus allgemein zugänglichen Inhalten (also z.B. Webseiten) „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich dadurch eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt". Hierfür bedürfe es einer Ermächtigungsgrundlage. Eine salvatorische Klausel, die viele Fragen aufwirft! S. aber auch den BMI-Entwurf zum Persönlichkeitsschutz (unten S. 140); dort wird jedoch auf „Geschäftsmäßigkeit" abgestellt.

61 BVerfGE 120, 274 (345).

heute in vielen Staaten und jedenfalls in Europa Gesetze, die dem Einzelnen das Recht garantieren, sich umfassend zu informieren. Die Behörden sind fast überall verpflichtet, ohne weitere Voraussetzungen jedem, der es wünscht, Einsicht in amtliche Unterlagen zu gewähren. Und über die gesetzlichen Verpflichtungen hinaus stellen heute alle möglichen Unternehmen und Behörden praktische, werbende und schlicht hilfreiche Informationen ins Netz ein; wir profitieren täglich davon. Wenn aber der Informationswunsch des einen mit dem Geheimhaltungswunsch des anderen kollidiert, sind wir wieder bei der Aufgabe, durch Abwägung eine Lösung zu finden.

Freilich sind in den Informationsfreiheitsgesetzen einige Fallgruppen ausgenommen (bei etwas unterschiedlicher Formulierung in den verschiedenen Ländern). Dass personenbezogene Daten, die dem Datenschutz unterliegen, nicht auf diesem Wege offenbart werden dürfen, ist selbstverständlich. Umstritten sind – verständlicher Weise – „Staatsgeheimnisse" und „Geschäftsgeheimnisse". Aber auch diese Vorbehalte standen schon in dem berühmten Freedom of Information Act von 1966, der zur Aufdeckung des Watergate-Skandals beigetragen hat. Die Fans von WikiLeaks und anderen „Offenbarungs"-Plattformen halten diese Schranken für obsolet, weil sie Staaten (Regierungen) und Unternehmen (Managern) nur Schlechtes unterstellen und das Heil von einer vollständigen Transparenz erwarten.

Nach den Informationsfreiheitsgesetzen (IFG) des Bundes und von elf Ländern hat jeder Anspruch darauf, dass die Verwaltung ihm ihre Akten offenlegt und Kopien gestattet. Das widerspricht nur scheinbar dem Datenschutz; denn die personenbezogenen Daten, die in der Verwaltung gespeichert werden, sind von dem Informationsanspruch ausgenommen. Die große Forderung nach Transparenz der Verwaltung ist also im Grunde bereits erfüllt; nur in fünf Bundesländern fehlt noch ein solches Gesetz. Den Katalog der Ausnahmen, der in allen Informationsfreiheitsgesetzen (auch des Auslands) ähnlich ist, finden freilich die „Piraten" aller Art viel zu umfangreich. Wer wie WikiLeaks auch militärische und diplomatische Geheimnisse veröffentlichen oder wer keine Rücksicht auf laufende Gerichtsverfahren nehmen will, dem erscheinen die Grenzen des Informationsanspruchs natürlich als zu eng gezogen. Der Gesetzgeber kann aber gar nicht anders als abzuwägen, welche Interessen der Allgemeinheit den Vorrang vor dem Informationswunsch Einzelner haben, und sei dieser Wunsch noch so gut „demokratisch" begründet. So ist es rechtspolitisch (jedenfalls im Grundsatz) nicht zu beanstanden, dass der Informationsanspruch nach dem Bundesgesetz in einer ganzen Reihe von Fällen nicht besteht, nämlich

„1. wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf

a) internationale Beziehungen,
b) militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr,
c) Belange der inneren oder der äußeren Sicherheit,
d) Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden,
e) Angelegenheiten der externen Finanzkontrolle,
f) Maßnahmen zum Schutz vor unerlaubtem Außenwirtschaftsverkehr,
g) die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitsrechtlicher oder disziplinarischer Ermittlungen,

2. wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann,
3. wenn und solange

a) die notwendige Vertraulichkeit internationaler Verhandlungen oder
b) die Beratungen von Behörden beeinträchtigt werden“ usw. (§ 3 IFG).

Das IFG schützt darüber hinaus auch den „behördlichen Entscheidungsprozess“ (§ 4), das geistige Eigentum sowie Betriebs- und Geschäftsgeheimnisse (§ 6). Die Beachtung schutzwürdiger Interessen Betroffener – also der Datenschutzaspekt – ist in § 5 IFG noch einmal ausdrücklich und differenziert geregelt

Über die Berechtigung einiger Spezialklauseln lässt sich streiten. Der Gesetzgeber wollte offensichtlich keine irgendwie „gefährliche“ Lücke lassen und hat daher manche Ausnahmen doppelt und dreifach festgelegt.[62] Hier wird sich gewiss noch einiges ändern, wenn die Beauftragten für die Informationsfreiheit mehr Fälle untersucht und Korrekturen angemahnt haben. Andererseits sind mehrere dieser Ausnahmen recht aktuell: Man denke nur an den Kampf gegen die Steuerhinterziehung und verbotene Kartelle (Nr. 1 d)) oder gegen die Ausfuhr von Rüstungsgütern in Konfliktzonen (Nr. 1 f)). Transparenz für die „Gegenseite“ wäre fatal für das Gemeinwohl. Dass strafrechtliche Ermittlungen oder die Abwehr von Gefahren bei voller Kenntnis der Beschuldigten und Verdächtigen nicht erfolgreich sein können, ist eigentlich selbstverständlich, aber auch in zivilrechtlichen Streitigkeiten und verwaltungsrechtlichen Planungen ist ein gewisses Maß an Beratungsgeheimnis zwingend erforderlich. Insiderwissen verführt in der Wirtschaft immer wieder zu Transaktionen zu Lasten Dritter; in der Verwaltung kann Ähnliches geschehen.

62 Vgl. etwa die Kommentierung von Schoch 2009, insbes. Vorb. zu §§ 3 bis 6, Rn. 29 ff. und Kommentar zu § 3 Rn. 206 ff.

Die Praxis tut sich mit den geltenden Gesetzen schwer; man versucht immer wieder, sie zu unterlaufen. Der Paradigmenwechsel vom Arkanprinzip – alles, was der Staat tut, wird zunächst einmal geheim gehalten – zum Öffentlichkeitsprinzip lässt sich nicht von einem Augenblick zum nächsten bewirken; es genügt nicht, den Hebel umzulegen, man muss auch Dampf machen, um das Schiff der Verwaltung auf den neuen Kurs zu bringen. Und das wird nur gelingen, wenn auch die Einzelheiten und die Ausnahmen klar und allgemein akzeptiert sind. Wer energisch genug nach bestimmten Unterlagen der Verwaltung sucht und notfalls die Gerichte um Hilfe ersucht, der hat durchaus eine Chance, sich gegen Verschleierungsversuche durchzusetzen. Die Gerichte sind zunehmend bereit, der Exekutive Grenzen zu setzen.

Grundrecht auf Internet?

Gibt es auch ein Grundrecht oder gar ein Menschenrecht auf Internet? So wie ein Grundrecht auf Datenschutz in verschiedene Länderverfassungen geschrieben wurde und auch immer wieder als Ergänzung des Grundgesetzes gefordert wird, werden auch Forderungen erhoben, dem Internet verfassungsrechtliche „Weihe" zu vermitteln. Die öffentliche Meinung neigt auch sonst dazu, einmal erreichte Rechtspositionen zu verfestigen und Reformvorschläge dadurch zu untermauern, dass sie als Konsequenz grundrechtlicher Freiheiten dargestellt werden. Daraus lässt sich dann wiederum ableiten, dass diese grundrechtliche Verankerung auch im Text der Verfassung ausdrücklich und speziell festgeschrieben werden müsse. Die Rechtswissenschaft stimmt solchen Forderungen häufig zu.

Das Bundesverfassungsgericht legt der Politik eine derartige Folgerungsweise nahe, indem es den Inhalt der Verfassung in „Leitsätzen" konkretisiert und insbesondere die Reichweite der Grundrechte genauer bestimmt. Seine verfassungsrechtlichen Argumentationen liefern immer wieder Munition für rechtspolitische Forderungen, die auf eine Verbesserung der Rechtsposition des Einzelnen hinauslaufen. Die politischen Kräfte, denen an einer bestimmten verfassungsrechtlichen Festlegung liegt, wollen damit verhindern, dass ein künftiges, anderes zusammengesetztes Parlament das Erreichte wieder rückgängig macht. Solange kein entsprechender Verfassungsrechtssatz gilt, so meinen viele, würde auch dem Verfassungsgericht die Macht zur Korrektur des Gesetzgebers genommen. (Tatsächlich würde das Gericht aber wohl zu entsprechenden Ableitungen aus anderen, allgemeineren Verfassungsnormen gelangen!).

Die populäre Methode der Verfassungspolitik weckt bei den meisten Menschen Vorstellungen und Erwartungen, die entweder schon wegen ihrer Einseitigkeit und Unausgewogenheit nicht realisiert werden können, oder aber solche, die bei ange-

messener Auslegung der Gesetze und der Verfassung auch ohne Verfassungsänderung begründet sind. Unrealistisch sind manche Forderungen, die Befugnisse von Polizei und Justiz so sehr zu reduzieren, dass sich jedermann in der Öffentlichkeit unerkannt bewegen kann.[63] Ein Beispiel für die andere Variante bildet die „Erfindung" des „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" durch das Bundesverfassungsgericht. In dem Urteil zur Unzulässigkeit der „Online-Durchsuchung" privater Computer[64] hat das Gericht dieses Recht als eine Ausprägung des allgemeinen Persönlichkeitsrechts bezeichnet, das seinerseits aus dem Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) in Verbindung mit dem Gebot der Achtung der Menschenwürde (Art. 1 Abs. 1 GG) hergeleitet wird. Die „Gewährleistung der Vertraulichkeit und Integrität" wird vielfach als ein „neues" Grundrecht, als eine besondere Form des verfassungsrechtlichen Individualschutzes aufgefasst, obwohl das juristische Ergebnis – Verfassungswidrigkeit des entsprechenden Landesgesetzes – auch ohne den neuen Begriff anerkannt werden müsste.[65] Es ist gewiss zweckmäßig, die Vielfalt der Phänomene durch eine differenzierte Begrifflichkeit zu ordnen, aber für die Betroffenen würde sich nichts ändern, wenn das Gericht die alten, bewährten Vorstellungen vom Persönlichkeitsschutz zugrunde gelegt und weiterentwickelt hätte. Übrigens haben einige Bundesländer ein Grundrecht auf Datenschutz in ihre Verfassungen aufgenommen; es ist nicht erkennbar, dass dort eine höhere Qualität oder Intensität von Datenschutz praktiziert wird als in den anderen Ländern.

Verfassungen sollen eigentlich kurz und knapp formuliert sein; sie sollen nicht Einzelfälle regeln, sondern nur die Grundstrukturen der Staatsorganisation und die Kernpositionen des Verhältnisses zwischen Staat und Individuen. Tatsächlich gehen viele Verfassungen weit über diese Grenzen hinaus, geben der Politik inhaltliche Richtlinien und versprechen den Einzelnen auch Schutz gegen gesellschaftliche Mächte. Damit prägen sie die Identität des Gemeinwesens und fördern – jedenfalls potentiell – die Integration der Menschen in den gemeinsamen Verband.

Aber eine Verfassung soll auch entwicklungsoffen sein; „sie muss politischen und gesellschaftlichen Akteuren Freiräume zu ihrer Entfaltung lassen, um dadurch Vielfalt zu sichern".[66] Auch aus diesem Grunde enthalten die Verfassungen viele relativ unbestimmte Formulierungen, die auf politischen Kompromissen beruhen und unterschiedlichen Interpretationen Raum lassen. Das bekannteste Beispiel der verfassungsrechtlichen Fixierung eines politischen Kompromisses ist der heutige Artikel 16 a des Grundgesetzes, der das Recht auf politisches Asyl – ursprünglich

63 In diese Richtung geht die „Verteidigung der Privaten" durch den Soziologen Wolfgang Sofsky (Sofsky 2007).
64 Urteil vom 20. Februar 2008, BVerfGE 120, 274
65 Zur juristischen Debatte vgl. u.a. Hoffmann-Riem 2009, S. 530 ff.; anders Bull 2011 a S. 34 f.
66 Voßkuhle 2011, S. XI/XII.

ein kurzer Satz in Artikel 16: „Politisch Verfolgte genießen Asylrecht“ – in vier umfangreichen Absätzen durch ein kompliziertes System von Detailregelungen, Ausnahmen und Gegenausnahmen ergänzt. Die Absicht, das Asylrecht vor der Abschaffung zu bewahren, ist verwirklicht worden, aber ob der Geist des alten Asylrechtssatzes, der als Einleitungssatz in Art. 16 a GG fortbesteht, erhalten worden ist, erscheint durchaus fraglich.

Kurz: Man darf von Verfassungsänderungen nicht zu viel erhoffen. Sie stellen in aller Regel den Abschluss einer Entwicklung dar, nicht deren Anfang (ausgenommen vielleicht so explizit zukunftsgerichtete Normen wie der Umweltschutz-Artikel 20 a des Grundgesetzes). Wenn die parlamentarischen Mehrheiten nicht ausreichen, um eine progressive Politik zu betreiben, hilft zwar unter günstigen Umständen das Bundesverfassungsgericht, aber auch dieses kann keine wirklichen Kehrtwendungen erzwingen.

Unter diesen Aspekten sind auch die Überlegungen zur verfassungsrechtlichen Verstärkung des Internets zu beurteilen. Soweit bloß plakativ von der „Freiheit *des* Internets“ gesprochen wird, ist schon unklar, wer denn da „frei“ sein soll; das Internet ist kein Zurechnungssubjekt, das Rechte oder Pflichten haben kann. Das Netz ist „stets nur Mittel zum Zweck“ (der freien Kommunikation) und steht eben deshalb nicht mit dem Kommunikationsgrundrecht auf gleicher Ebene.[67] Ein Anspruch auf *Zugang zum* Internet ist immerhin vorstellbar, und es wird berichtet, dass bereits ein großer Teil der Bevölkerung diesen Zugang für ein Grundrecht hält.[68] Gemeint ist aber auch ein Recht auf „freie Entfaltung *im* Internet“ und vor allem auf Abwehr aller staatlichen Eingriffe in die Nutzung des Internets.[69] Ohne dass das Grundgesetz geändert werden müsste, ist schon jetzt ein starkes „Recht auf Internet“ gesichert – nicht als Anspruch eines jeden Menschen auf unentgeltlichen Zugang zum jeweils modernsten weltweiten Netz und nicht als Recht auf beliebige Äußerungen im Netz, wohl aber als eine Pflicht des Staates zur Gewährleistung einer ausreichenden Infrastruktur und – im Rahmen des Möglichen – als gesetzlicher Anspruch des Einzelnen auf diskriminierungsfreie *Teilhabe* an dieser Infrastruktur, vor allem aber als verfassungsrechtliches *Abwehrrecht* gegen Einschränkungen der Meinungs-, Medien-, Kunst- und Wissenschaftsfreiheit.[70] Kai von Lewinski hat in aller wünschenswerten Klarheit herausgearbeitet, dass es keiner verfassungsrechtlichen „Operation“ (in Gestalt einer Verfassungsänderung)

67 So Hofmann 2012 in einem Bericht über einen Meinungsstreit in der New York Times.

68 Lewinski 2011, S. 70 Fn. 1 m.w.N.

69 Der Gutachter des DJT versteht „Internetfreiheit“ als ein „Institutsgrundrecht“ ähnlich der Presse- und Rundfunkfreiheit: „Sich Äußernde im Internet und erst recht Intermediäre“ müssten „sich auf die Institutsgrundrechte, insbesondere das der ‚elektronischen‘ Presse berufen können“ (Spindler 2012, S. 27 und 133).

70 Weitergehend fordert z.B. Spindler eine „allgemeine Freiheit der Internetdienste“ (Spindler 2011, S. 28), während Dix für eine Erweiterung der Medienfreiheiten nach Art. 5 GG „keinen Anlass“ sieht (in: DJT 2012, S. 72 These 13.

bedarf, um die vermeintlichen Lücken im Grundgesetz zu schließen, sondern dass zur Korrektur der altersbedingten „Kurzsichtigkeit“ unserer Verfassung eine „gesetzliche Sehhilfe“ genügt: „Dem ‚Recht auf Internet‘ ist mittelfristig am besten gedient, wenn man die Interpretationsspielräume des Grundgesetzes nutzt“.[71] „Das bloße textliche Einfügen eines ‚Rechts auf Internet“ ist (politische) Geschmacksfrage“.[72] Die Einführung einer *Universaldienstleistungspflicht* (also der von der Bundesnetzagentur festgelegten Pflicht eines Unternehmens, in einem bestimmten Gebiet für technisch hochwertige Verbindungen zu sorgen)[73], wie sie z.B. von der SPD vorgeschlagen wird, dürfte praktisch bedeutsamer und effektiver sein als die Diskussion über ein neues Grundrecht.

Wenn demgegenüber eingewandt wird, nur eine ausdrückliche verfassungsrechtliche Verankerung der Internet-Freiheit sei eine ausreichende Bastion gegen Unterdrückungsabsichten der Regierungen, so ist zu entgegnen: Gegen rechtsfeindliche Bestrebungen von Regierenden kommt kein Verfassungstext an. Die Geschichte liefert bis zum heutigen Tag genügend Beispiele dafür, wie rücksichtlos Machthaber mit Verfassungen umgehen, wenn sie ihren Absichten im Wege stehen.[74] Auch wenn das Bundesverfassungsgericht die politischen Mehrheiten in wichtigen Fällen mit Erfolg korrigiert hat – der Gesetzgeber könnte mit verfassungsändernder Mehrheit auch diese Urteile korrigieren. In wirklich entscheidenden Machtproben hängt die Verteidigung der rechtsstaatlichen Grundwerte ohnehin davon ab, dass das Volk selbst sich zur Wehr setzt und die Medien den Mut aufbringen, den Mächtigen zu widersprechen. Solange die Demokratie funktioniert, wird uns diese Probe erspart bleiben.

Das vermeintliche Ende der Privatheit

Niemand will für seine Umgebung ein „offenes Buch“ sein, jeder und jede will seine und ihre Geheimnisse für sich behalten. Deshalb will auch niemand für andere „transparent“ sein; kein anderer Mensch soll ihm oder ihr in die Seele schauen können. Wir sträuben uns instinktiv dagegen, anderen zu tiefen Einblick in unsere Gedanken und Wünsche zu geben; wir fürchten, zum „gläsernen“ Menschen zu werden. So verteidigen wir unsere räumliche und ideelle „Privatsphäre“ oder – in etwas umfassenderer Formulierung „Privatheit“ (dieser Begriff wird meist synonym gebraucht). Geradezu abschreckend finden wir es, wenn sich Dritte daran machen, „Persönlichkeitsprofile“ herzustellen, die zur Grundlage von Entschei-

71 Lewinski 2011, S. 92.
72 Lewinski 2011, S. 94.
73 Vgl. dazu §§ 78 ff. Telekommunikationsgesetz.
74 So auch Heller 2011, S. 160 (s. unten S. 63 ff.).

dungen werden können, ohne dass wir uns dazu äußern können. Auch wer „nichts zu verbergen hat“, empfindet Unbehagen, wenn andere versuchen, in fremde Seelen einzudringen.

Tatsächlich ist es mit dem Schutz vor diesem Eindringen schlecht bestellt – wenn man den Äußerungen von Experten und Journalisten folgt, die sich kritisch mit der Entwicklung der Informationstechnik und ihrer Anwendung befassen. Datenschützer haben Schreckensbilder vom drohenden oder bereits erreichten „Überwachungsstaat“ gemalt; auch ich habe während meiner Amtszeit als Bundesbeauftragter für den Datenschutz diese Gefahr betont und dafür geworben, dass Staat und Gesellschaft mit personenbezogenen Daten rücksichtsvoll umgehen. Das Bewusstsein für die Notwendigkeit von Datenschutz ist durch diese Öffentlichkeitsarbeit ständig gewachsen, aber die Öffentlichkeit hat nicht nachvollzogen, dass viele der Sorgen sich als unbegründet erwiesen haben. Das Scheitern der Volkszählung 1983 gilt als Nachweis der gewachsenen Einsicht in die Risiken der Informationstechnik (zu Unrecht, denn gerade bei dieser Massen-Datenverarbeitungsaktion war das Risiko extrem gering!).[75] Nach wie vor wird der vermeintlich mutige Boykott der harmlosen Volkszählung als demokratische Höchstleistung gefeiert, und man vermisst eine gleiche Fundamentalkritik gegenüber aktuellen informationstechnischen Neuerungen. Das Internet aber gilt als der stärkste Feind der Privatsphäre, und wegen seiner Allgegenwärtigkeit meinen inzwischen viele, ein wirksamer Schutz der Privatsphäre sei endgültig unmöglich geworden. Der Buchtitel „Das Ende der Privatsphäre“[76] wird als Tatsachenfeststellung verstanden; was der Autor – der amtierende Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – als Mahnung zur Umkehr verstanden wissen will, wird als abgeschlossener Prozess angesehen. Romanschriftsteller beteiligen sich in der Nachfolge von George Orwell an der politischen Debatte mit Horrorszenarien über ein künftiges Alltagsleben unter allumfassender Überwachung.[77] „Die Privatsphäre ist ein Auslaufmodell“; „Wir treten ein in das Zeitalter der ‚Post-Privacy‘: in ein Leben nach der Privatsphäre“, heißt es in dem Buch eines Bloggers und Filmkritikers unter Bezugnahme auf die alarmistischen Titel anderer Bücher, wenn auch mit einer ganz anderen Schlussfolgerung (auf die ich zurückkommen werde).[78]

75 Mehr dazu: Bull 2012, S. 151 ff.
76 Schaar 2007.
77 S. etwa Trojanow/Zeh in Anknüpfung an Sofsky; dazu die kritische Rezension von Milos Vec, FAZ v. 14.9.2009, S. 8 .
78 Heller 2011.

Tatsachen und Legenden

Um die phantastische Erfindung des weltweiten Netzes ranken sich manche Legenden. Sie sind zum großen Teil durch tatsächlich bestehende Eigenschaften der verwendeten Technik, wirtschaftliche Strukturen und soziale (sozialpsychologische) Gesetzmäßigkeiten begründet. Aber sie werden in einem Maße verallgemeinert, dass sie schließlich mit der Realität nichts mehr zu tun haben. So ist es gewiss richtig, dass im Netz unendlich viele Informationen über einen großen Teil der Menschheit gespeichert sind, aber es ist falsch, dass „das Netz" „alles" „über jeden von uns" „weiß". Abgesehen davon, dass „das Netz" kein Subjekt ist, sondern dass in Wahrheit nur die großen Technikfirmen, Netzbetreiber und Diensteanbieter gemeint sind, also das Oligopol von Microsoft, Google, Facebook, Twitter und einigen weiteren Unternehmen – die irreführende Verallgemeinerung liegt in der Behauptung, dass die Herren des Netzes die gleiche Art von „Wissen" besäßen wie natürliche Personen. Es wird unterstellt, dass die Verfügung über die Speichermedien und Computer gleichzusetzen sei mit dem Bewusstsein von Individuen.

Die anthropomorphen Begriffe und Metaphern, die durch die Internet-Debatte geistern,[79] verschleiern den entscheidenden Unterschied: Der Computer hat kein Bewusstsein und kein Gedächtnis.[80] Er speichert Zeichen, die nach unseren Konventionen Inhalte repräsentieren, und verändert oder transportiert sie nach vorgegebenen Programmen. Aus den Zeichen entsteht Bedeutung erst durch das Bewusstsein, und dieses ist dem Menschen vorbehalten; der Maschine fehlt es. Es ist ein langer Weg, ehe aus den Zeichen und Datenträgern zunächst „Information" und im günstigen Fall „Wissen" wird – und noch länger ist der Weg zu der Macht, von der man annimmt, das Wissen vermittle sie. Zwar können die technischen Vorgänge, die aus den Zeichen etwas „Bedeutendes" machen, sehr schnell vor sich gehen, aber die Wahrnehmung durch menschliche Augen oder Ohren und die Verarbeitung im menschlichen Kopf können lange dauern; unter Umständen brechen diese Vorgänge ergebnislos ab.

Unser Unbehagen angesichts der undurchschaubaren Apparate, das „diffuse Gefühl des Ausgeliefertseins"[81] rührt zum guten Teil daher, dass wir uns dieser wesentlichen Eigenschaften des technischen Systems nicht bewusst sind. Wir fragen uns zum Beispiel im Hinblick auf Standortsuchsysteme: „Wer weiß eigentlich,

79 Kritisch zum Gebrauch von Metaphern auch Passig/Lobo 2012, S. 36 ff., 48.

80 Auch dies wird von einigen Autoren inzwischen bestritten, das Gegenteil zumindest als Zukunftsvision behauptet. Vgl. etwa Meckel 2012 („Hybridisierung des Menschen durch die Verbindung von Körper, Technik und Geist"); Metzinger 2012 („Erste Maschinen mit Bewusstsein werden unglücklich sein"). Der britische „Experte" David Levy soll „perfekte Sexroboter" angekündigt haben und mit der „ersten Heirat zwischen Mensch und Maschine" „so in 50 Jahren" rechnen (Weber 2012). Auf derartige Phantasien kann keine Politik gegründet werden.

81 Kurz/ Rieger 2011, S. 8.

wo ich mich gerade befinde? Und warum weiß er auch, wo meine Freunde gerade sind – sogar besser als ich?“[82] Die Antwort ist ganz einfach: „Er“ ist nicht irgendeine Person oder Personengruppe, sondern das dazu eingerichtete und programmierte Datenverarbeitungssystem. Dieses unpersönliche Konstrukt „weiß“ natürlich gar nichts; es hält nur die Daten bereit, aus denen jemand Informationen ableiten kann. Um das unheimliche Äußere der Technik zu überwinden, personalisieren wir den Computer, und diese metaphorische Ausdrucksweise lenkt uns von der einfachen Wahrheit ab, dass die Geräte im Kern so viel und so wenig leisten wie ihre Benutzer, nur schneller und zuverlässiger, und dass ihr „Wissen“ immer erst von einem Menschen aktiviert werden muss (z.B. weil jemand nach mir sucht – sei es aus gutem, sei es aus schlechtem Grunde, aber nie ohne Anlass).

Wenn das technische Gehirn „abschaltet“, zu langsam oder falsch reagiert, gehen die Zeichen und ihre Bedeutung vorzeitig ganz oder teilweise verloren. Im Übrigen können die gespeicherten Informationen zwar theoretisch noch lange aktiviert werden, aber solange das nicht geschieht, sind sie nicht Bestandteile „unseres“ Gedächtnisses. Wir sprechen zwar auch von Archiven und Aktensammlungen als „Gedächtnis“ der Gesellschaft, doch auch das ist bloß metaphorisch gemeint und in gewisser Hinsicht schief.

Das Gedächtnis der Computer und die Lücken im Netz

Eine andere Behauptung lautet: Das Internet vergisst nichts. Auch das ist in dieser Pauschalität falsch. „Auch wenn es Internetarchive gibt: Wer einmal versucht hat, eine bestimmte Webseite aus dem Jahr 1998 noch einmal aufzurufen, kann das bestätigen“.[83] Richtig ist, dass ein großer Teil der Speicherungen dauerhaft ist und auch verfügbar bleibt. Daten können tatsächlich eine Langzeitwirkung entfalten; man staunt oft, dass uralte, längst überholte Angaben in irgendeinem Speicher „überlebt“ haben, während die Welt darum herum sich verändert hat. „Jugendsünden“ können Greise einholen. Äußerungen, die ich selbst vergessen habe oder für gelöscht halte, werden aus den Tiefen des Netzes hervorgezogen und dem Betroffenen vorgehalten – ob es ihm lieb ist oder nicht.

Andererseits braucht man sich nur klar zu machen, wie viele Daten tagtäglich von den speichernden Stellen wieder gelöscht werden. Große Mengen personenbezogener Daten werden gelöscht, weil dies gesetzlich vorgeschrieben ist – man denke an die Überprüfungs- und Löschungspflichten der Sicherheitsbehörden (die bisweilen – offline, weil diese Daten gar nicht im Netz stehen – sogar übereifrig

82 Kurz/Rieger 2011, S. 8.
83 Drösser 2011. Ebenso Passig/Lobo 2012, S. 45 („ein Narrativ, das … wenig mit den Fakten zu tun hat“).

befolgt werden, wie im Fall einiger Unterlagen über den „Nationalsozialistischen Untergrund“). Unternehmen löschen ständig Daten, weil sie den Speicherplatz anders verwenden wollen, und die Kosten dauerhafter Aufbewahrung dürften auch die Betreiber der sozialen Netzwerke dazu veranlassen, die Daten ihrer „Mitglieder“ und Nutzer nach einiger Zeit zu vernichten. Die an den Daten interessierten werbenden Unternehmen wollen „frische Daten“; mit archivwürdigen Angaben können sie nicht viel anfangen. Wer an der Vergangenheit bestimmter Personen interessiert ist – z. B. als alter Freund oder Konkurrent, als Behörde oder als potentieller Arbeitgeber – kann zwar manches Relevante im Netz recherchieren, aber niemals sicher sein, dass er ein auch nur halbwegs vollständiges und aktuelles Persönlichkeitsbild des Betreffenden erhält. Polizei und Justiz recherchieren selbstverständlich auf vielerlei Wegen und möglichst gezielt, also unter Kriterien, die aus konkreten Verdachtsanlässen abgeleitet sind; sie verlassen sich nicht allein auf die Internetspuren.

Es gehört zu den allgemeinen Pflichten nach dem Datenschutzrecht, unrichtige Daten zu berichtigen, nicht mehr erforderliche und unzulässig gespeicherte Daten zu löschen und bestrittene Angaben zumindest zu sperren. Die Gesetze können zwar kein „Recht auf Vergessen“ begründen – denn das Vergessen kann nur in den Köpfen der Menschen stattfinden, auf die kein Gesetz Einfluss hat. Aber Löschungspflichten sollen dazu beitragen, dass Altes und Falsches nicht dauerhaft weitergetragen wird. Nach dem Entwurf einer Datenschutz-Grundverordnung der EU soll jeder Betroffene ein „Recht auf Vergessenwerden und auf Löschung“ haben (so die Überschrift des einschlägigen Artikels).[84] Die umfassende Umsetzung dieses Anspruchs wird allerdings schwierig sein.[85]

Der Einzelne hinterlässt bei jeder Suche im Internet Spuren und bei jeder Eingabe personenbezogene Daten, die zunächst gespeichert werden und vielfältig genutzt werden können; aus diesen Angaben kann ein Mosaik zusammengesetzt werden, das viel über Verhaltensweisen und Kaufpräferenzen, Aufenthalte und Lebensgewohnheiten verrät.[86] Dass damit „Persönlichkeitsprofile“ hergestellt würden, die für gute wie böse Zwecke nutzbar seien, ist eine der wesentlichen Ursachen für die Angst, die viele – wirklich oder angeblich – vor der Informationstechnik empfinden. Aber was auch immer Psychologen und Werbestrategen aus den Internetspuren der Nutzer herausholen, sie können nichts Zuverlässiges über die Absichten und Meinungen der Einzelnen aussagen. Zu einem wirklichen Persönlichkeitsprofil aber würde gerade das „forum internum“, die innere Bewusstseinsver-

84 Art. 17 des Entwurfs (Kommissions-Drucksache (2012) 11 v. 25.1.2012.
85 Die technische Lösung in Gestalt des „digitalen Radiergummis“ scheint nicht praktikabel zu sein, vgl. Drössel 2011.
86 Mehr dazu unten S. 65 f.

fassung des einzelnen Menschen gehören. Der „Datenschatten", die „digitale Identität"[87] unterscheidet sich von dem wirklichen Menschen.

Schließlich trifft auch die Behauptung nicht zu, der Staat und/oder die Wirtschaft wollten „alle" Informationen über „alle" Einwohner zur Kenntnis nehmen oder zur Verfügung haben.[88] Es kennzeichnet gerade das geltende Recht, dass die Befugnisse zur Speicherung, Verarbeitung und Verwendung persönlicher Daten durch eine Vielzahl spezieller Rechtsnormen geregelt sind, und es ist eine unbewiesene Behauptung, dass diese Normen ständig verletzt würden. Sie werden im Großen und Ganzen eingehalten. Dass damit immer noch eine riesige Zahl von Datenübermittlungen zulässig ist, kann keiner bestreiten, aber nur wer sich aus der Gesellschaft verabschieden will, kann den Austausch und die Nutzung von Informationen grundsätzlich ablehnen.

Zur Klarstellung: Mit der Kritik der Internetlegenden soll nicht etwa bestritten werden, dass es zahlreiche Risiken des Datenmissbrauchs gibt. Aber für die rechtliche Bewältigung der neuen Probleme ist es nicht hilfreich, sich an den Verallgemeinerungen auszurichten. Vielmehr muss es eine Rolle spielen, wie häufig ein Phänomen ist und wie viele Menschen es tatsächlich betrifft. Sonst werden die Normen, mit denen das Risiko bekämpft werden soll, zu weit geschnitten, und stiften dann mehr Schaden als Nutzen.

Ich räume ein: Diese Betrachtungsweise setzt ihrerseits die Gewissheit voraus, dass meine Gedanken trotz aller Computer und Netze letztlich frei sind und frei bleiben, selbst wenn andere versuchen, meine Lebensäußerungen auszudeuten. Wer dies bestreitet, kommt zu anderen Schlüssen. Die Politik muss und will auch auf diese andere Wahrnehmung eingehen und auch die Menschen „abholen" und zufrieden stellen, denen die Technik unheimlich bleibt.

Die Dimensionen des Persönlichkeitsschutzes

Damit sind wir bei der Frage, wie das Recht auf die Tatsachen, aber auch auf die Ängste der Menschen eingehen soll. Der übliche Ansatzpunkt ist das tradierte und verfassungsrechtlich geschützte Persönlichkeitsrecht. Kulturkritiker behaupten, das Zeitalter des Privatsphärenschutzes sei vergangen, und im günstigsten Fall plädieren sie dafür, aus der „Post-Privacy" das Beste zu machen.[89]

Über den Inhalt der Begriffe „Privatheit" und „Privatsphäre" besteht – entgegen dem ersten Anschein – kein Konsens. Seine Bedeutung schwankt zwischen „Robinson" und „My home is my castle", zwischen vollständiger Abschottung des

87 Diese Begriffe verwenden z.B. Worms/Gusy 2012, S. 95.
88 Auch diese Vorstellung wird vielfach verbreitet, vgl. etwa Sofsky 2007; Bolz 2010.
89 Heller 2011, S. 7 f.

Einzelnen von der Gesellschaft und dem Schutz eines räumlich abgegrenzten Bereichs. Privatheit ist Voraussetzung von Freiheit; sie ist Kraftquelle und Erholungsraum. Es ist trotzdem falsch, sie einfach mit Freiheit gleichzusetzen. Innere Freiheit, wie sie im privaten Bereich gewonnen und ausgeübt wird, reicht für die Entfaltung des Menschen nicht aus; Freiheit muss sich gerade in der Auseinandersetzung mit anderen bewähren.

Die Extremposition: Abschirmung von der Gesellschaft

Es ist zwar durchaus richtig, wenn gesagt wird, Privatheit sei „zuerst ‚Freiheit von' und nicht ‚Freiheit zu etwas'", und für die private Freiheit sei „primär" „die Abwesenheit von Zwang und äußerer Einwirkung". [90] Aber damit ist eben nur die eine Seite des Themas angesprochen und die andere, eigentlich unübersehbare ist ausgeblendet. So verschanzt sich der Soziologe Sofsky in seiner „Zitadelle der persönlichen Freiheit", die er als Schutz nicht nur vor „Enteignung und Entmündigung", sondern auch vor „Aufdringlichkeit und Bevormundung, vor Macht und Zwang" ansieht.[91] Er legt Wert auf „Abstand" und wittert „Einmischung" von der gesamten Umwelt: „Das Heer der Eindringlinge reicht von besorgten Eltern, misstrauischen Verwandten und neugierigen Nachbarn über selbsternannte Moralprediger, Toleranzprüfer, ehrgeizige Meinungsmacher und Gesinnungspädagogen bis zu den Steuereintreibern, Spitzeln und Wachposten der Fürsorge". „Sie alle", meint der Autor, „verstoßen gegen das Freiheitsrecht des einzelnen, in Ruhe gelassen zu werden".[92]

Nicht alle „Verteidiger des Privaten" gehen in ihrer Soziophobie so weit. Man darf vermuten, dass auch die „Robinsoniaer" gern an den Segnungen der Zivilisation teilhaben möchten, die Wirtschaft, Technik und Staat geschaffen haben, und dafür gewisse „Einmischungen" der sozialen Umwelt hinnehmen. Doch scheinen viele zu glauben, alle Leistungen anderer und der Gemeinschaft genießen zu können, ohne dafür selbst irgendetwas über sich selbst preiszugeben. Selbst Robinson auf seiner einsamen Insel hätte aber eine Hilfsbitte mit der Angabe seines Standortes verbunden (wenn er ihn denn bezeichnen konnte), und in der Flaschenpost hätte er zumindest seinen dringendsten Bedarf beschrieben. Und dass die gemeinsame Organisation zur Erfüllung öffentlicher Aufgaben, die wir Staat nennen, nicht ohne Steuern auskommt und soziale Wohltaten nicht anonym verteilt werden können, sollte zum soziologischen Grundwissen gehören. Es führt in die Sackgasse,

90 Sofsky 2007, S. 153.
91 Sofsky 2007, S. 37. Dieser Autor bestreitet die Friedensfunktion des Rechts und spricht in negativem Sinne von „totalem Rechtsstaat" (S. 24).
92 Sofsky 2007, S. 37 f.

wenn dem Staat, der die Konflikte mit seinen Mitteln lösen will, nur Unterdrückungsabsicht unterstellt wird.[93]

„Öffentlich“ gegen „privat“

Die Abgrenzung zwischen „privat“ und „öffentlich“ ist seit je ein zentrales Thema der politischen Theorie und der Rechtswissenschaft. Zu einer freiheitlichen Ordnung gehört sowohl Privatheit wie Öffentlichkeit: die Abschirmung einer privaten Sphäre und die Freiheit privater Betätigung wie auch die öffentliche Wahrnehmung und öffentliche Kritik des individuellen Handelns. Die Grenzen des Privatheitsschutzes und des Öffentlichkeitsanspruchs variieren im historischen und internationalen Vergleich. „Privatheit ist eine kulturelle Konstruktion“; „die Grenzen des Privaten gelten als konstitutiv für das normative Selbstverständnis moderner, liberal-demokratischer Gesellschaften und sind doch notorisch umstritten“.[94] Und die Bestimmung dieser Grenzen geschieht durch Rechtsnormen: „Es bedarf des Rechts“.[95]

Das geltende Recht erkennt den menschlichen Wunsch nach Intransparenz an, und zwar überall in der westlichen Welt und weit darüber hinaus, und so gelten in Deutschland wie in ganz Europa, in den USA und Kanada und in vielen anderen Staaten, auch auf anderen Kontinenten Rechtsnormen, die es anderen erschweren sollen, die geheimen Gefühle und Sehnsüchte der Menschen herauszufinden.[96] Sie sind teils Richterrecht, teils Gesetzesrecht, und über ihre richtige Anwendung wird lebhaft diskutiert. Die Europäische Menschenrechtskonvention hat schon 1952 das Recht jeder Person auf „Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ statuiert,[97] und die Charta der Grundrechte der Europäischen Union hat diese Bestimmung fast wörtlich übernommen[98] und ein Recht auf Schutz der personenbezogenen Daten hinzugefügt.[99]

93 So aber Sofsky 2007, u.a. S. 38.
94 Seubert 2012, S. 101. S. a. die Beiträge in Seubert/Niesen (Hrsg.) 2010.
95 Worms/Gusy 2012, S. 96.
96 Die umfassende Literatur und Rechtsprechung zum Persönlichkeitsschutz kann hier nicht zitiert werden; das ist auch nicht nötig, weil die Grundlinien unumstritten sind. Die unterschiedlichen Formen des Persönlichkeitsschutzes werden im folgenden Text durchgesprochen.
97 Art. 8 EMRK.
98 In Art. 7 EU-Grundrechte-Charta heißt es nur statt „Korrespondenz“ „Kommunikation“.
99 Art. 8 EU-Grundrechte-Charta.

Würde, Freiheit, Selbstbestimmung

Während der Schutz der Privatheit bei uns – in Deutschland und seinen europäischen Nachbarstaaten – im Kern auf das Gebot der *Menschenwürde* zurückgeführt wird, betrachten amerikanische Juristen und Politiker den Gedanken des Datenschutzes als Konsequenz der *Freiheit* des Individuums.[100] Der Yale-Professor James Q. Whitman hat dies in einem materialreichen rechtsvergleichenden Aufsatz auf die Formel von den „Two Western Cultures of Privacy" gebracht, deren Grundvorstellungen „Dignity versus Liberty" sind.[101] Andreas Zielcke plädiert in seiner Besprechung dieses Ansatzes dafür, die beiden Ideale aufeinander zu beziehen und miteinander zu verbinden; sonst blieben zu große Lücken im Rechtsschutz,[102] und das hat viel für sich – auch wenn die amerikanische Nüchternheit in manchen Zusammenhängen deutlich mehr Klarheit schafft als der deutsche Griff zu den moralischen Sternen.

Zwischen Freiheitsrecht und Menschenwürde schlägt die Idee der *Selbstbestimmung* eine Brücke, und diese Idee spielt in der deutschen Literatur und Praxis eine wichtige Rolle. Selbstbestimmung über das, was ich anderen über mich mitteilen will, ist eine rechtliche Selbstverständlichkeit. Ich kann bestimmen, wem ich was über mich offenbare. Ich kann Schutz davor verlangen, genötigt, bedroht, getäuscht oder unter Drogen gesetzt zu werden. Vom Staat kann ich erwarten, dass er nur diejenigen Informationen über mich sammelt und verwertet, die er zur Erfüllung seiner Aufgaben benötigt. Als soziales Wesen kann ich allerdings nur begrenzt darüber bestimmen, was andere über mich wissen; ich kann nicht verhindern, dass andere sich ein (aus meiner Sicht) falsches Bild von mir machen. Das Recht, über meine Äußerungen selbst zu bestimmen, ist von Wissenschaft und Gerichten zum „informationellen Selbstbestimmungsrecht" weiterentwickelt worden. Vom Bundesverfassungsgericht zum Bestandteil des Grundgesetzes erklärt, bildet es seit drei Jahrzehnten den rechtstechnischen Rahmen für die richterliche Ausformung des Datenschutzes und wird von Verwaltung und Wirtschaft, aber auch von der Wissenschaft als Eckpfeiler der Informationsrechtsordnung immer neu beschworen.

Der Schritt von der Äußerungsfreiheit zur „informationellen Selbstbestimmung" ist freilich größer als man zunächst annehmen mag. Denn diese juristische Weiterentwicklung wird im Grunde den Besonderheiten gerade der Informationssammlung und des Kommunikationswesens nicht gerecht. Sie kann allenfalls eine Richtungsangabe darstellen („möglichst viel Selbstbestimmung beim Umgang mit den Daten"), ist aber zu formal, als dass sie eine Abgrenzung zwischen erlaubtem

100 Zielcke 2010 mit Hinweis auf Whitman 2004
101 Whitman 2004.
102 Zielcke 2010.

und verbotenem Verhalten ermöglichen und inhaltliche Ansätze zur Konfliktlösung liefern könnte.[103]

Die Selbstbestimmungsidee führt immerhin zur praktischen Lösung eines Teils der Probleme, indem sie die *Einwilligung* der Betroffenen zur Erlaubnisgrundlage macht. Wann eine Einwilligung sinnvoll ist (und wann das Gesetz eine allgemein verbindliche Lösung schaffen muss), und unter welchen Umständen die Einwilligung wirksam sein soll, kann und muss seinerseits rechtlich geregelt werden.[104] Wenn die Einwilligung vorab nicht erlangt werden kann – wie bei den Geodatendiensten (Google Street View u.a.) –, kann die Selbstbestimmung immerhin nachträglich durch ein möglichst leicht zugängliches Widerspruchsrecht gewährleistet werden.[105]

Die Geschichte des Persönlichkeitsrechts

„Entdeckt" wurde die „Privatheit" von US-amerikanischen Juristen; als Ursprung aller weiteren juristischen Überlegungen zu diesem Themenfeld gilt der Aufsatz der Bostoner Juristen Samuel D. Warren und Louis D. Brandeis „The Right to Privacy" aus dem Jahre 1890.[106] Die Autoren reagierten damit auf die in der Presse aufkommenden Sensationsgeschichten aus dem Privatleben Prominenter; sie folgerten den Schutz der Betroffenen aus dem ungeschriebenen Common Law, das sich „in seiner ewigen Jugend" immer weiter entwickle. Das Recht auf Leben werde nunmehr auch als das Recht verstanden, „sich des Lebens zu freuen – das Recht in Ruhe gelassen zu werden".[107] Trotz der etwas schwachen Begründung setzte sich nach längeren Schwankungen die Ansicht durch, dass es ein solches Recht auf Privatheit gebe und dass seine Verletzung zum Schadensersatz verpflichte. Die Presse war davon nicht gerade begeistert.

In Deutschland herrschte bis nach dem Zweiten Weltkrieg die Meinung vor, nur die Ehre und das Ansehen einer Person seien rechtlich geschützt. Ein *allgemeines Persönlichkeitsrecht* erkannte der Bundesgerichtshof erstmals 1958 an; es billigte einem Herrenreiter, dessen Foto zur Werbung für ein Stärkungsmittel missbraucht worden war, einen Schadensersatzanspruch wegen Verletzung dieses Rechts an.[108] Im Laufe der Zeit konstruierten die Gerichte ein ganzes System von Rechts-

103 Zur Kritik des „informationellen Selbstbestimmungsrechts" vgl. Bull 2011 a m.w.N.; s.a. Schoch 2012.
104 Vorschläge dazu zuletzt bei Spindler 2012. Zu den Rahmenbedingungen s.a. Wolf Osthaus, in: DJT 2012, S. 75, Thesen 8-10 (u.a.: Abnutzungs- und Gewöhnungsgefahr, falsche Anreize).
105 Spindler 2012, S. 134 These 21.
106 Warren/Brandeis 1890. Näheres bei Bull 1984, S. 77 ff.
107 Das Wort vom „right to be let alone" hatte bereits der Richter Cooley geprägt.
108 BGHZ 26, 349. Vgl. nochmals Bull 1984, S. 79 ff.

positionen – vom *Recht auf das eigene Bild*[109] über das *Recht an der eigenen Stimme* bzw. *am gesprochenen Wort*[110] bis zum *Recht an den „eigenen" Daten* (das freilich nur im übertragenen Sinne gemeint ist)[111]. Man knüpfte an den Schutz der *räumlichen* Privatsphäre an, die durch die Unverletzlichkeit der Wohnung (Art. 13 GG) besonders gesichert ist, und erweiterte den Privatsphärenschutz um den Bereich der privaten *Geheimnisse*; von da aus war der Schritt zu den sonstigen Informationen über die eigenen Verhältnisse nicht weit.

Klassisch ist etwa die Formulierung des Bundesverfassungsgerichts, dem Einzelnen müsse „um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein ‚Innenraum' verbleiben", „in dem er ‚sich selbst besitzt' und ‚in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt'".[112] Im konkreten Fall ging es darum, ob die Bürger im Rahmen eines Mikrozensus nach ihren Urlaubsgewohnheiten gefragt werden durften. Das Verfassungsgericht hat das gebilligt, weil die Statistiker sich nur für „das Verhalten des Menschen in der Außenwelt" interessierten; der „unantastbare Bereich privater Lebensgestaltung" werde dadurch nicht erfasst. Zitiert wird aus diesem Urteil meist nur die über den eher harmlosen Gegenstand weit hinausgreifende Formulierung, dass es dem Staat verboten ist, „den Menschen 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".

Heute wird „Privatheit" oder „Privatsphäre" fast schon allgemein mit „Datenschutz" gleichgesetzt, und die eine wie die andere Rechtsfigur wird zusätzlich mit der Achtung vor der Menschenwürde begründet. Wir sollten aber genauer unterscheiden; denn die Schutzrichtung ist nicht identisch, und es ist nicht selbstverständlich, dass etwa die Offenbarung von Geheimnissen aus der Privat- oder Intimsphäre nach den gleichen Rechtsnormen beurteilt wird wie die Veröffentlichung irgendwelcher Lebenssachverhalte im Netz. Die Menschenwürde ist verletzt, wenn ein Individuum erniedrigt, missachtet, wie eine Sache behandelt wird. Schwere Beleidigungen können diesen Tatbestand erfüllen, aber nicht jede Missachtung ei-

109 Vgl. § 22 Kunsturhebergesetz und § 201 a StGB sowie u. v. a. etwa die Entscheidungen des BVerfG und des EGMR in Auseinandersetzungen verschiedener illustrierter Blätter mit dem Ehepaar von Hannover („Caroline"-Entscheidungen), insbes. Beschluss des BVerfG v. 26.2.2008, BVerfGE 120, 180 und Urteil des EGMR v. 7.2.2012, Kommunikation & Recht 2012, S. 179.

110 Aus der Rspr.: BGHZ 27, 284 (290); BVerfGE 34, 238 (grundsätzliches Verbot heimlicher Tonbandaufnahmen) und 106, 28 (39ff.) (Verbot einer Mithöreinrichtung, die ohne Wissen des Gesprächspartners eingerichtet wurde).

111 BVerfGE 65, 1 (43).

112 BVerfGE 27, 6 (mit Zitaten aus: Wintrich, Die Problematik der Grundrechte, 1957, S. 15 f., und Dürig, in: Maunz/Dürig/Herzog/Scholz, Grundgesetz, 2. Aufl., Art. 1 Rdnr. 37).

ner Datenschutzvorschrift. Mit Datenschutznormen lässt sich die Verletzung individueller Rechte bekämpfen, aber nicht die Praxis, dass rechtmäßig gewonnene Daten über Individuen wie Waren gehandelt und ausgewertet werden. Ausufernde Datenverarbeitung, massenhafte Speicherung und technikgestützte Auswertung von Lebensäußerungen sind Phänomene, die viele beunruhigen – aber sind das wirklich Angriffe auf Grundrechte oder gar auf die Menschenwürde von Individuen? Doch allenfalls dann, wenn Menschen missachtet, respektlos behandelt, in ihrer Integrität verletzt werden. Das aber ist bei nüchterner Betrachtung der meisten Vorgänge von Massendatenverarbeitung nicht der Fall. Die „Täter“ interessieren sich nicht für die individuell Betroffenen, sie behandeln nicht die Personen, sondern die diese betreffenden Daten wie Sachen, und bilden Gruppen von Betroffenen, die nicht mehr als Individuen gemeint sind, sondern als Träger bestimmter Merkmale. Die Betroffenen haben kein „Eigentum“ an den „personenbezogenen“ Daten, und selbst wenn sie es hätten, würden wir den „Diebstahl“ von Daten nicht als Angriff auf die Würde der Eigentümer ansehen.

Von „Verwaltung“ zu „Verdatung“

Irgendwann im Laufe der frühen Diskussionen um die Risiken der Datenverarbeitung ist das Wort von der „Verdatung“ aufgekommen. So wie die Menschen „verwaltet“, „verkabelt“ und „vernetzt“ werden – was immer auch eine Form von Unterlegenheit ausdrückt –, werden die Individuen in Ansammlungen von Daten verwandelt, also zum *Objekt fremder Verfügung* gemacht. Das aber könnte in der Tat mit der Achtung vor der Menschenwürde unvereinbar sein.

Entscheidend dafür, ob die Verarbeitung persönlicher Informationen eine unzulässige „Verdatung“ bedeutet, ist die Situation, in die der Betroffene durch diesen Vorgang gerät.[113] Entweder wird nur etwas über ihn von einer Behörde oder einem Unternehmen zur Kenntnis genommen und es werden Schlüsse daraus gezogen – das ist bei jeder Form von „Verwaltung“ im weitesten Sinne unvermeidlich; es ist auch gewollt, weil ja aufgrund der Informationen etwas geschehen soll. Die typischen Fälle sind, dass der Betroffene einen Anspruch auf eine Leistung oder Zahlung hat – zu diesem Zweck werden im Geschäftsleben die meisten Daten erhoben und verwendet – oder dass andere oder der Staat eine Leistung von ihm verlangen können – seien es Steuern, Sozialabgaben, private Schadensersatz- oder Unterhaltszahlungen und was sonst noch an Gegenständen privaten oder staatlichen Interesses in Betracht kommt. Die unvermeidliche Folge aber ist die Unterwerfung des Einzelnen unter die Macht Dritter: Die Information kann im Streitfall gegen

113 In einem anderen Sinn benutzt Heller (2011, S. 54 ff.) den Begriff der Verdatung („die Verdatung der Welt, der Texte, der Menschen“).

den Einzelnen verwendet werden. Ist es also eine unerlaubte „Verdatung", ein Fall von Unterdrückung des Individuums, wenn dem Gläubiger zur Durchsetzung eines Anspruchs auf Schadensersatz das Recht zugesprochen wird, die dazu erforderlichen Daten über den Schuldner zu verwenden?

Betrachten wir ein paar Beispiele, bei denen von Unterwerfung des Individuums durch den Staat oder durch Private (insbesondere Unternehmen) gesprochen wird. Die schwersten Eingriffe in die Sphäre des Einzelnen gehen von den Behörden aus, die zur Verfolgung von Straftaten und zur Bekämpfung von Gefahren für die öffentlichen Sicherheit berufen sind: Polizei, Staatsanwaltschaften und Geheimdienste (Verfassungsschutzämter, Bundesnachrichtendienst und militärischer Abschirmdienst). Verfolgt die Justiz mit Hilfe der Polizei Straftäter, so darf sie aufgrund gesetzlicher Regelungen zahlreiche Informationen sammeln und auswerten, untereinander abgleichen und zur Überprüfung an weitere Behörden übermitteln. Die Beteiligten sind an die Strafprozessordnung und die Polizeigesetze gebunden (die übrigens deutlich weniger Befugnisse haben als die beliebten Fernsehkommissare in Anspruch nehmen, aber doch eine ganze Menge). Es ist unvermeidlich, dass einzelne Akteure versuchen, ihre Befugnisse zu überschreiten, sei es aus Übereifer, sei es aus Nachlässigkeit oder weil sie die Rechtsnormen falsch interpretieren. Den Betroffenen können daraus große Belastungen erwachsen; wer zu Unrecht strafrechtlich verfolgt wird, fürchtet aus gutem Grund, dass „immer etwas hängen bleibt". Und dabei ist es häufig ganz unerheblich, ob die Informationen in einem Computer gesammelt wurden oder ob jemand ein Gerücht verbreitet hat, das nur in einigen Köpfen existierte. Ja, die Beeinträchtigung kann viel größer sein, wenn ein Staatsanwalt ohne Benutzung einer Datensammlung jemanden einer Straftat bezichtigt, als wenn er im Zuge einer Rasterfahndung alle Angehörigen einer bestimmten Personengruppe überprüft. Man denke an einige Fälle öffentlichen „Prangers", etwa die Verhaftung eines Verdächtigen vor laufenden Fernsehkameras oder die vorzeitige Bekanntmachung eines Ermittlungsverfahrens.

Dennoch: Gefahren für das persönliche Ansehen, für die Ehre oder für die berufliche Entwicklung bestehen besonders da, wo große Mengen von Informationen automatisiert verarbeitet werden, und insbesondere da, wo sie zu Zwecken der öffentlichen Sicherheit verwendet werden. Man gerät eher in Verdacht – zu Recht oder zu Unrecht, man wird leichter übervorteilt oder übertölpelt, wenn andere einen besonders großen Bestand an Informationen nutzen können.

Klar ist: Die „Online-Durchsuchung" privat genutzter Computer durch eine Behörde beeinträchtigt die Privatsphäre noch mehr als eine Wohnungsdurchsuchung und Beschlagnahme von Akten. Von der Wirtschaft gehen solche Gefahren nicht aus; kein Unternehmen kann uns etwas vorschreiben. Aber wenn Unternehmen mehr Informationen besitzen als ihnen in einem ausgewogenen Verhältnis zustehen, droht den Unterlegenen Diskriminierung, vor allem durch Verweigerung von

Vertragsabschlüssen und Krediten. Es ist unbestritten, dass das Recht gegen solche Nachteile schützen muss.

Der Schutz der freien und unbefangenen Kommunikation

Über die Abwehr konkreter Schäden hinaus soll das Persönlichkeitsrecht aber auch dazu beitragen, dass wir weiterhin *frei* und *unbefangen* miteinander *kommunizieren* können. Die Freiheit und Unbefangenheit der Kommunikation ist von vielen Seiten bedroht, aber in höchst unterschiedlicher Intensität: von Seiten des Staates durch unmittelbare Eingriffe, Verbote und Sperren, von Privaten durch Ausspähung, durch Auswertung vorhandener Daten und durch unerwünschte Ansprache. Man tauscht sich nicht offen aus, wenn man befürchten muss, dass Fremde mithören oder mitlesen. Man will nicht mit Leuten in Verbindung stehen, die man nicht kennt, denen man nicht vertraut. So wird Datenschutz auch als Schutz vor unerwünschter Kommunikation verstanden – und sogar als Schutz davor, von Fremden angesprochen zu werden oder namentlich adressierte Sendungen zu erhalten.

Nach weitverbreiteter Ansicht liegt eine Beeinträchtigung der individuellen Freiheit schon dann vor, wenn die Menschen das *Gefühl* bekommen, sie würden ständig beobachtet, registriert, bewertet und kontrolliert. Wenn ich so frage, habe ich allerdings den Maßstab gewechselt; es geht dann nicht um die tatsächliche Wirkung der Informationsprozesse, sondern um deren subjektive, durch Vermutungen und Ängste verzerrte oder übersteigerte Wahrnehmung. Ist das ein hinreichend fester Boden dafür, die betreffende Form von Datenverarbeitung einzuschränken oder gar zu unterbinden? Habe ich ein *Grundrecht auf* den *Respekt* anderer – oder ist das nicht vielmehr nur eine *gesellschaftliche* Norm, eine Regel des anständigen Umgangs miteinander, die den Staat nichts angeht? Immerhin nehmen die nationalen und europäischen Gesetzgeber auch solche Ängste zum Anlass, regelnd auf die Entwicklung der Internet-Kommunikation einzuwirken. Ein Großteil der Auseinandersetzungen mit den sozialen Netzwerken dürfte gerade um die Frage kreisen, wie weit dieser „Gefühlsschutz“ gehen soll oder darf. Praktikable Abgrenzungen können aber – wenn überhaupt – nur die Gesetzgeber formulieren; es ist unmöglich, solche Regeln aus den Grund- und Menschenrechten unmittelbar abzuleiten.

Das Grundmuster der Risikodiskussion

Möglichkeit und Wirklichkeit der Techniknutzung

Bei der Beschäftigung mit dem Themenkreis „Gesellschaft und Technik" fällt immer wieder auf, dass *technische Möglichkeiten* den Ausgangs- und Endpunkt von Diskussionen über *politische und soziale Probleme* bilden. Viele Probleme werden als Folge technischer Entwicklungen angesprochen, und neue Techniken werden als Lösung angeboten. Es ist zwar verständlich, wenn Unternehmen der Internetwirtschaft so vorgehen; sie brauchen Geschäftsmodelle und Marketingstrategien. Politik und Wissenschaft jedoch erfüllen ihre Aufgaben nicht ausreichend, wenn sie nur von dem ausgehen, was die Technik-Erfinder und Vermarkter versprechen, statt umgekehrt zunächst die wahrscheinliche Entwicklung zu erforschen, die Interessenlage zu klären und um politische, soziale, wirtschaftliche und rechtliche Lösungen zu ringen. Die Technik muss dabei einerseits als eine Bedingung der sozialen und ökonomischen Entwicklung bedacht werden, andererseits aber als (anzupassendes!) Hilfsmittel gestaltet werden. Ob z.B. die neuen Medien wirklich soziale Strukturen verändern, wie häufig behauptet wird, ist keineswegs sicher und hängt u.U. gerade umgekehrt von der rechtlichen Ausgestaltung ab, um die in den netzpolitischen Diskussionen gerade gestritten wird. Man sollte das Pferd nicht vom Schwanze her aufzäumen.

Regelmäßig läuft die Untersuchung der Gefahren der Informationstechnik in einer bestimmten Form ab.[114] Über welche neue Technik und welche Nutzungsart auch immer geredet und geschrieben wird – die Kontroverse ist immer gleichartig strukturiert. Den Befürwortern stehen die Kritiker gegenüber, und ihre Bedenken laufen immer auf dieselbe Begründung hinaus:

- Erstens: Es sei *möglich*, dass die Technik für unerwünschte Zwecke benutzt werde,
- es sei zweitens auch *wahrscheinlich*, dass tatsächlich in der Zukunft jemand (der Staat, ein Unternehmen, Private) versuchen werde, dies zu tun, so dass
- drittens ein ernstes Risiko bestehe, dass durch Fehlhandlungen und Fehlentwicklungen tatsächlich *Schäden* bei Betroffenen entstehen.

In allen drei Punkten wird regelmäßig zu pauschal und ohne ausreichende empirische Basis argumentiert. Staatliche Maßnahmen, insbesondere neue Gesetze müssen auf eine solidere Grundlage gestellt werden als auf nicht zu Ende gedachte Prognosen und gefühlte Bedrohungen.

114 Dass „fast alle Elemente der heutigen Datenschutzdiskussion" schon vor Jahrzehnten in Gebrauch waren, dokumentieren Passig/Lobo 2012 (S. 201 ff.) an alten Presseartikeln.

Es macht schon einen großen Unterschied aus, nach welchem *Maßstab* ein Handlungszweck unerwünscht ist. Der beliebte Begriff „Missbrauch" kann bedeuten, dass Daten unter *Verletzung von Rechtsnormen* gesammelt und genutzt werden – dann ist die Sache klar. Es kann aber auch sein, dass nur Verstöße gegen *Moralgesetze* oder Leitlinien der *Sozialethik* (z.B. der Wirtschaftsethik) befürchtet werden. Diese wiegen deutlich geringer als Rechtsverletzungen, jedenfalls ist die Durchsetzung rein ethischer Maßstäbe nicht primär Aufgabe des Staates, sondern Sache der Gesellschaft. Noch geringeres Gewicht hat die Besorgnis, dass nur gegen Regeln des gesellschaftlichen *Anstandes*, des *Takts* und der *Höflichkeit* verstoßen werde (also z. B. jemand taktlos oder ungeschickt angesprochen wird); das ist nicht strafbar und nicht einmal gesetzlich verboten, sondern allenfalls von der Gesellschaft missbilligt und für die Betroffenen lästig. „Missbrauch" von Daten ist also durchaus nicht in jedem Fall ein Skandal.[115]

Prominente Bürgerrechtler verweisen in solchen Diskussionen gern darauf, dass der Datenschutz aus dem obersten Gebot der Verfassung hergeleitet wird, nämlich aus dem Gebot, die Menschenwürde zu achten und zu schützen (Art. 1 Abs. 1 Grundgesetz). Diese Verknüpfung – die, wie gesagt, eine Besonderheit unserer Rechtsordnung darstellt – müsste eigentlich jedem die Augen dafür öffnen, dass gerade nicht jede Verletzung einer Datenschutznorm zugleich eine Missachtung des höchsten Verfassungsgebots darstellen kann; die Datenschutznorm ist möglicherweise ihrerseits überzogen, so dass sie das hohe Gut der Menschenwürde in allzu „kleine Münze" zerteilt und damit letztlich entwertet.

Der recht häufig vorkommende umgekehrte Schluss – weil der Datenschutz in Art. 1 Abs. 1 Grundgesetz verankert sei, sei mit jeder Einbuße an Datenschutz auch das Grundgesetz betroffen – mag zwar logisch erscheinen, ist aber für die rechtliche und politische Gewichtung sozialer Vorgänge geradezu irreführend. Schutz der Menschenwürde bedeutet Verbot der Folter, der Erniedrigung von Menschen, ihrer Bloßstellung und Knebelung. Auf den Schutz personenbezogener Daten wird die Menschenwürde-Formel mit einem sprachlichen Kunstgriff[116] ausgedehnt: Man sagt, der Mensch werde auch durch den Gebrauch seiner Daten „zum Objekt gemacht", und meint damit nicht nur die Unterwerfung unter den Willen eines ande-

115 Der Skandal liegt allerdings häufig darin, dass aus irgendwelchen Informationen falsche, unsichere oder verleumderische Schlüsse gezogen werden, die ihrerseits nicht begründet sind, oder dass Kontrahenten, Konkurrenten und Neider eine Person mit Informationen konfrontieren bzw. öffentlich diskreditieren, die nach Maßstäben des Rechts längst verjährt und in amtlichen Registern getilgt wären. Solche Vorgänge können durch noch so perfekte Vorschriften über den Umgang mit den Daten kaum verhindert werden. Man denke an die üblichen Verdächtigungen gegen mehr oder minder prominente Mitmenschen, die durch Indiskretionen oder Spekulationen befördert werden.

116 Und unter Vernachlässigung des Umstandes, dass der Persönlichkeitsschutz von den Gerichten aus dem allgemeinen Freiheitsrecht (Art. 2 Abs. 1 GG) *in Verbindung mit* Art. 1 Abs. 1 GG hergeleitet worden ist. Es geht also gar nicht um die „reine" Menschenwürde.

ren, sondern auch die unter ein Computerprogramm, mit dessen Hilfe andere den Einzelnen beeinflussen, eben die schon besprochene „Verdatung".

Das hat natürlich eine gewisse Plausibilität für sich, aber überzeugend ist es nur, wenn die Bezugnahme auf das höchste Verfassungsgebot durch Tatsachen gerechtfertigt ist. Die Kritiker blenden die Realität weitgehend aus, wenn sie auf der zweiten Stufe ihrer Argumentation regelmäßig behaupten: „Alles was möglich ist, wird tatsächlich realisiert". Hier kommt nun ein tiefsitzendes Misstrauen zum Ausdruck. Dieses Misstrauen gilt heute als Ausweis wahrer Liberalität; es grassiert nicht nur unter Anhängern der FDP, sondern ist in vielen Parteien präsent und beeinflusst auch die Entscheidungen von Parlamenten, Regierungen und Gerichten. Es geht zwar nicht so weit wie die Grundauffassung vieler US-amerikanischer Republikaner, dass alles schlecht sei, was der Staat anstelle der Einzelnen tut, aber es führt doch dazu, dass den staatlichen Stellen alles Schlechte zugetraut und alles Gute nur von der Gesellschaft, vom Volk erwartet wird. Diese moralische Zweiteilung der Welt ist naiv und behindert den Fortschritt. (Sie wird übrigens in dem Augenblick wieder aufgegeben, in dem auch die Gesellschaft zweigeteilt wird, nämlich in „gute" Individuen und „böse" Großunternehmen, gegen deren Macht wiederum der Staat helfen muss.)

Eine besondere Ironie der Geschichte liegt darin, dass die Bürgerrechtler, die besonders nachdrücklich auf die möglichen Gefährdungen der Individualrechte hinweisen, im Grunde nicht anders argumentieren als jene Vertreter der Sicherheitsbehörden, die ihre Ermittlungskompetenzen möglichst weit ins „Vorfeld" des Verbotenen ausdehnen wollen: Sie wollen ihrerseits rechtliche Schranken schon im „Vorfeld" des verbotenen Umgangs mit Daten errichten, damit potentielle Daten-„Sünder" gar nicht erst in Versuchung geraten können (und nehmen in Kauf, dass die dafür nötigen Schranken für die normale, rechtmäßige Datennutzung zu hoch werden). Die Kriminalisten wollen Informationen über die kriminelle „Szene", aus denen sie auf mögliche künftige Straftaten schließen können, um im konkreten Fall besser gerüstet zu sein; sie misstrauen ihrer eigenen Fähigkeit, geschehene Verbrechen ohne solche Vorfeldinformationen aufzuklären (und übersehen, dass die erforderlichen Informationen aus der Privatsphäre der Betroffenen stammen). Die Bürgerrechtler misstrauen den Behörden – und erst recht den Bürgern; denn sie halten es für ungewiss, ob die eindeutigen Verbote und Gebote (z.B.: bestimmte Informationen nicht an Arbeitgeber oder Vermieter und Polizei oder Verfassungsschutz weiterzugeben) eingehalten werden. „Sicher ist sicher" ist insofern das gemeinsame Motto von Datenschützern und Datenverarbeitern.

Zwei Beispiele für Risiko-Phantasien

An zwei Beispielen soll gezeigt werden, wie professionelle Datenschützer die Risiken beschreiben, die angeblich durch neue Techniken oder neue Methoden der Datenverarbeitung entstehen: das „Selbstmordwarnsystem" von Facebook und das schon einmal erwähnte Smart Metering.

Das Warnsystem, von dem die Rede ist, soll dazu dienen, dass Facebook-Mitgliedern, die in ihren Kontakten mit Freunden eine Suizidabsicht erkennen lassen, auf Hilfsangebote hingewiesen werden. Wer von einem Freund als selbstmordgefährdet gemeldet wird, erhält (nach einer Prüfung durch einen Facebook-Mitarbeiter) eine Nachricht mit der Aufforderung, sich Hilfe zu holen; die Telefonnummern von Hilfsorganisationen wie der Telefonseelsorge sind beigefügt. Eine Datenschutz-Beamtin soll dazu nach einem Zeitungsbericht in kritischer Absicht gesagt haben: Es sei „denkbar, dass Facebook genau für diejenigen, die in einer Lebenskrise stecken, entsprechende Werbung schaltet oder auch entsprechende Werbung nicht schaltet, also etwa keine Lebensversicherungen bewirbt".[117] Dass diese Möglichkeit als ein Risiko für einen Selbstmordgefährdeten angesehen wird, das durch rechtliche Regeln ausgeschlossen werden müsse, ist grotesk.

Durch das genaue Messen des Energieverbrauchs von Haushaltsgeräten soll nach verbreiteter Ansicht das Recht auf informationelle Selbstbestimmung gefährdet sein, außerdem auch die Unverletzlichkeit der Wohnung und das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, das „Computer-Grundrecht".[118] Metaphorisch werden die angeblichen Gefahren mit Begriffen aus der Optik beschrieben: Die Informationen bildeten einen „Datenschatten", eine „immer präzisere Abbildung" unserer Aktivitäten vom TV-Konsum über das Babywickeln bis zum nächtlichen Toilettengang; oder: unsere häuslichen Handlungen „spiegeln" sich vermeintlich im Stromverbrauch.[119] Wie das geschehen soll, wird in allgemeinen Wendungen umschrieben: die sensiblen Informationen „lassen sich gewinnen", heißt es, die Daten seien „interpretationsfähig", oder es wird einfach von der „Aussagekraft" der Daten gesprochen. Tatsächlich handelt es sich bei all diesen Interpretationen – die ganze Hefte von Fachzeitschriften füllen – stets um die gleichen Spekulationen: Man unterstellt aufgrund sehr schlichter Alltagserfahrungen, dass der oder die Bewohner sich in dieser oder jener Weise verhalten, wenn sie Haushaltsgeräte, Fernseher, Computer oder andere Stromverbraucher anstellen oder angestellt lassen. Davor, dass diese „Erkenntnisse" zur Überwachung der Bewohner genutzt werden, müssen diese nach der Ansicht der Beobachter geschützt werden. Dass ich aber in Wahrheit vielleicht gar nicht zusehe, wenn der Fernseher

117 Frisse 2012.
118 Hornung/Fuchs 2012, S. 21.
119 BfDI 2011, 57. S. a. Müller 2010; Roßnagel/Jandt 2010.

läuft, dass ich das Licht versehentlich oder absichtlich brennen lasse oder dass ich nachts lese, statt zu schlafen, dass man also etwas ganz anderes tut als die stromverbrauchenden Geräte ihrem Zweck gemäß zu nutzen, kommt nicht in den Blick. Selbst wenn es so ist, wie angenommen, wenn also die Bewohner zu bestimmten Zeiten das TV-Gerät anschalten und zu anderen ausschalten, ist nicht erkennbar, welche Schlüsse daraus die potentiellen Überwacher ziehen mögen. Natürlich möchte ich im Allgemeinen nicht, dass andere erfahren, welche Fernsehprogramme ich bevorzuge oder wann ich nachts aufstehe. Aber wen interessiert das wirklich?

Der einzig „harte Kern" all dieser Spekulationen ist die Sorge, dass Einbrecher meinen können, das Haus sei unbewohnt, wenn längere Zeit kein Strom oder Gas verbraucht wird. Auch dann besteht eine ernst zu nehmende Gefahr nur unter der Bedingung, dass die Verbrauchsdaten zeitnah einer kriminellen Szene zugänglich werden – was durch angemessene Datensicherung weitgehend verhindert werden kann. Ein anderes Schreckgespenst ist „der Versicherungsvertreter an der Haustür", der als belästigend empfunden wird; für ihn seien die Verbrauchsdaten „lukrativ im Beratungsgeschäft rund um Energieeffizienz" – [120] aber wo ist hier die Gefahr, der man mit den Mitteln des Rechts begegnen müsste? Schließlich wird befürchtet, dass Ermittlungsbehörden derartige Daten eines Tages auswerten könnten – aber warum sollte dieses (individuell sehr geringe) Risiko der rechtsstaatlich geordneten Strafverfolgung ausgeschlossen werden? Staatsanwaltschaften, Polizei und Justiz sind an die Strafprozessordnung gebunden; sie sind überdies geschult darin, Verdachtsmomente gezielt zu erarbeiten und nicht etwa pauschalen Spekulationen zu folgen. Die Datenschutzvorschriften im Energiewirtschaftsgesetz[121] reichen jedenfalls aus, die Daten vor der normalen Neugierde Dritter abzuschirmen und die phantasievollen Gefahrenszenarios zu verhindern.

Misstrauen auf allen Ebenen

Erstaunlicherweise hat sich gerade auch das Bundesverfassungsgericht dabei hervorgetan, die Missbrauchsmöglichkeiten aufzuzeigen, die aus mehrdeutigen oder zu weit gefassten Gesetzesbegriffen erwachsen. Ohne empirische Nachweise hat das oberste Gericht mehrfach ausgemalt, was alles mit den gesammelten Daten geschehen könne, wenn Beamte ihre Befugnisse extensiv auslegen.

So hat man sich vorgestellt, dass die Kfz-Kennzeichen, die von automatischen Erfassungsgeräten der Polizei gelesen und für Fahndungszwecke ausgewertet werden dürfen, mit anderen Daten verknüpft und dann dazu benutzt werden könnten, „Informationen über einen ganzen Kriminalitätsbereich, das Umfeld, die ‚Szene'

120 Heckmann 2011 a, S. 3.
121 § 21 g EnWG mit Rechtsverordnungsermächtigung in § 21 i Abs. 1 Nr. 4.

und den gesellschaftlichen Hintergrund zu sammeln" – also auch über „einen Personenkreis, der durch sein Verhalten keinen Anlass für die Aufnahme in den Fahndungsbestand gegeben hat".[122] Weil das im Gesetz angeblich nicht klar genug ausgedrückt war, hat das Gericht die Befugnis annulliert, überhaupt Lesegeräte zu benutzen.

Den Kern der Begründung des Urteils zur Kfz-Kennzeichenerfassung bildet die Sorge, durch die „vielfältigen Nutzungs- und Verknüpfungsmöglichkeiten" könnten „weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können".[123] Die Richter ziehen ihrerseits „Schlüsse", ohne sich und den Lesern klar zu machen, ob denn die „möglichen" Nutzungen und Verknüpfungen zulässig wären und auf welche Weise sich Eingriffe „anschließen" sollten. Ich muss es wiederholen: Das Bundesverfassungsgericht misstraut den handelnden Beamten; es vermutet letztlich, diese würden ihre Amtspflicht verletzen, sich gesetzeskonform zu verhalten und ihre Kompetenzen nicht nur formal einzuhalten, sondern auch den Sinn und Zweck der Befugnisnormen zu beachten. Für ein Gericht ist das eine befremdliche Einstellung. Seine Aufgabe ist nicht, über Möglichkeiten zu spekulieren, sondern das Recht durchzusetzen, und zwar gerade auch gegen sinnwidrige extensive Auslegung, gegen eine Praxis, die den Grundsatz der Verhältnismäßigkeit missachtet. Wie eigenwillig diese Rechtsprechung ist, ergibt sich auch daraus, dass das Gericht die Befugnisnorm gebilligt hätte, wenn sie nur detaillierter formuliert gewesen wäre. Der freiheitsfördernde Effekt dieser Judikatur verpufft also, wenn der Gesetzgeber immer kompliziertere Vorschriften erlässt!

Das Misstrauen mancher Beobachter gegen die Datenverarbeitung der Behörden geht so weit, dass sogar die Stelle des Bundes, die der Sicherheit in der Informationstechnik dienen soll, als potentielle Überwachungsinstanz angesehen wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem Gesetz sorgfältig eingegrenzte Befugnisse. Es darf u.a. die „Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist".[124] Die automatisierte Auswertung muss „unverzüglich" erfolgen, und die Daten müssen „nach erfolgtem Abgleich sofort und spurenlos gelöscht werden".[125] Seitenlange Detailvorschriften sollen sicherstellen, dass die Daten wirklich nur für den gesetzlichen Zweck ver-

122 BVerfGE 120, 378 (410 f.).
123 BVerfGE 120, 378 (398).
124 § 5 Abs. 1 Satz 1 Nr. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) v. 14. 8. 2009 (BGBl. I S. 2821).
125 § 5 Abs. 1 Satz 2 BSI-Gesetz.

wendet werden. Nun aber liest man, dass zwei prominente „Datenschützer“ (ein Bundestagsabgeordneter und ein freiberuflich tätiger Experte) meinen, diese Daten dürften nicht ohne „konkreten Anlass“ aufgezeichnet werden. Denn dabei könne „beispielsweise ermittelt werden, wer sich auf dem Internetportal der Bundeszentrale für gesundheitliche Aufklärung über Impotenz informiert hat“. Was um Himmels willen werden die Datensicherheits-Experten des BSI mit dieser Information anfangen? Stellen sich die Beschwerdeführer wirklich vor, irgendjemand werde die zu Kontrollzwecken gespeicherten Daten aus privater Neugierde durchsehen und etwa damit rechnen, einen Bekannten mit solch einer Information blamieren oder lächerlich machen zu können? Nachdem sie mit dieser Beschwerde beim Bundesverfassungsgericht nicht zum Erfolg gekommen sind, haben sie jetzt den Europäischen Gerichtshof für Menschenrechte angerufen.[126] Man sollte das ohnehin überlastete Straßburger Menschenrechtsgericht nicht mit derart weltfremden Klagen behelligen.

Die Sorge, dass die Beamten ihre Rechte extrem weit interpretieren oder gar überschreiten würden, findet sich freilich auch bei einigen Insidern. Manche trauen ihren Kollegen sehr wohl zu, sich über rechtliche Grenzen hinwegzusetzen, sobald die Gelegenheit günstig ist. „Ich kenne meine Pappenheimer“, sagt einer, der jahrelang als Kriminalbeamter gearbeitet hat und heute einen anderen Beruf ausübt, nachdem er sich bei den Kollegen durch liberale Ansichten unbeliebt gemacht hat. Andere Kenner der Sicherheitsbehörden erblicken dort ebenfalls ein großes Maß an Jagdeifer und manchmal ein zu geringes Maß an rechtlichen Skrupeln.

Gemeinsam ist vielen Zweiflern also, dass sie Rechtsverletzungen von großem Gewicht nicht nur für möglich, sondern sogar für wahrscheinlich halten. Viele übersehen jedoch, dass der tatsächliche Eintritt von Grenzüberschreitungen noch von einer weiteren Bedingung abhängig ist, nämlich von fehlender Abschreckung und erfolgloser *Kontrolle*. Die Akteure der Datenverarbeitung sind in das dichte Netz der Datenschutzbestimmungen eingebunden; sie sind der Aufsicht unabhängiger Datenschutzbeauftragter unterworfen und müssen ihre Handlungen gegenüber Aufsichtsbehörden und Gerichten verantworten – ganz zu schweigen von der Kontrolle durch die Medien, die von vielen mehr gefürchtet werden als die Justiz.

Es ist verzeihlich, wenn jemand, der die Technikentwicklung allein aus der Perspektive des Informatikers oder Elektronikers verfolgt, die technische Machbarkeit mit der Verwirklichung von Rechtsverletzungen gleichsetzt. Einen solchen Kurzschluss sollte sich aber niemand leisten, der regelmäßig soziale, wirtschaftliche und politische Vorgänge beurteilt. Manager und Beamte, Journalisten und Sozialwissenschaftler wissen, dass es viele Faktoren sind, die das Verhalten der Menschen bestimmen. Sie sollten die *Interessenlage* der Akteure realistisch einschätzen und

126 Bericht (dapd) in der Süddeutschen Zeitung vom 25. 1. 2012.

überlegen, wie hoch für diese selbst das Risiko ist, wegen Pflichtwidrigkeiten bestraft, vielleicht sogar aus dem Dienst entfernt zu werden.

Wenn man sich z.B. vorstellt, Polizeibeamte könnten systematisch die Telekommunikations-Verbindungsdaten einzelner Personen „auf eigene Rechnung" zu Lasten der Betroffenen „vermarkten", also etwa „Dossiers" und „Bewegungsprofile" bestimmter Mitmenschen herstellen und an private Interessenten verkaufen, wird man auf den Gedanken kommen, dass es dazu eines Kreises potentieller Käufer bedarf. Schon diese Bedingung dürfte nicht ganz einfach zu erfüllen sein. Ein Interesse Außenstehender ist zwar vorstellbar, und sei es, dass jemand auf diese Weise klären will, ob sein zukünftiger Schwiegersohn eine „weiße Weste" hat. Belastende Informationen können für Konkurrenten und Nebenbuhler wertvoll sein. Aber es dürfte schwierig sein, einen ertragreichen Markt für solche Informationen aufzubauen – schwieriger jedenfalls als etwa illegal mit Waffen zu handeln. Dass der Informationshandel aber über kurz oder lang von den korrekt handelnden Kollegen entdeckt und aufgelöst werden wird, ist schon deshalb ziemlich sicher, weil Abfragen aus dem Polizeicomputer automatisch dokumentiert werden. Die illegalen Datenhändler müssten mit der Entlassung rechnen. Es ist tatsächlich schon vorgekommen, dass pflichtvergessene Beamte persönliche Daten aus polizeilichen Beständen „privat" an Dritte gegeben haben, um ihnen gefällig zu sein oder weil ihnen dafür Geld geboten wurde. Sie wurden bestraft, und niemand behauptet, solche Fälle seien typisch für die ganze Polizei.

Gesetze werden nicht dadurch unbrauchbar, dass viele gegen sie verstoßen – im Gegenteil! Wäre dem so, hätten wir das Strafgesetzbuch und viele andere Normen längst abschaffen (oder durch wesentlich schärfere Gebote ersetzen!) müssen. Gleichwohl ist es ein beliebtes Argumentationsmuster, dass wegen der Möglichkeit von Rechtsverstößen die Nutzbarkeit von Datensammlungen eingeschränkt werden sollte. Aus Angst vor dem Fehlgebrauch wollen viele den normalen Gebrauch von Dateien bis zur Unzumutbarkeit erschweren.

Die Beschwörung des Unrechtsstaates

Die äußerste Form dieser Argumentation besteht in der Beschwörung eines diktatorischen Regimes, das alle bisherigen Sicherungen über den Haufen wirft. Wenn die Diskussion zu der Feststellung gelangt ist, dass die Risiken von Missbrauch und Pflichtverstößen in unserem heutigen Staat begrenzt und beherrschbar sind, erscheint prompt auf dem Podium das Extremargument: Wir dürfen einer künftigen autoritären, rechtsfeindlichen Regierung nicht die Mittel in die Hand geben, uns vollständig zu unterdrücken. Haben nicht die Nazis die Einwohnerkarteien, Personenstandsregister und Kirchenbücher zur Judenverfolgung genutzt? Hat nicht die

DDR ein technikgestütztes Informationssystem über alle aufgebaut, die der kritischen Distanz zur herrschenden Partei verdächtig waren? Nutzen nicht Diktatoren zunehmend das Internet, um geheime Opposition aufzudecken und zu zerschlagen?

Ja, das ist alles richtig – und doch einseitig und unvollständig.[127] Die Nationalsozialisten waren schon im Besitz der Macht, als sie ihre Verfolgungen begannen, und ihre „Machtergreifung" war durch andere Faktoren begünstigt als gerade durch Technik. Die Technik, die von der Stasi benutzt wurde, war nach heutigen Maßstäben unzureichend. Aber das MfS hatte reichlich menschliche Mitarbeiter, die das Volk mit ganz konventionellen Methoden ausspionierten und Dissidenten denunzierten. Geht man in der Geschichte weiter zurück, kommt man zu dem Schluss, dass die Herrscher zwar von der Entwicklung der Waffentechnik profitierten, dass sie aber bei der Unterdrückung ihrer Völker sogar ohne Schreibmaschine und Drucker auskamen. Diktaturen entstehen nicht, weil es perfekte Informationssysteme gibt, sondern weil handgreiflich Gewalt ausgeübt wird, weil die Menschen die Demokratie nicht energisch genug verteidigen oder weil sie von den Machthabern bestochen werden. Man lese die Literatur über das Ende der Weimarer Republik; da finden sich reichlich Belege für diese These.

Selbst wenn man die Bedeutung der Technik stärker gewichtet: Solange wir in rechtsstaatlichen Verhältnissen leben und auf absehbare Zeit keine Revolution zu erwarten ist, wäre ein Verzicht auf die Nutzung von Informationstechnik nicht zu rechtfertigen. Nicht nur Informationstechnik, sondern viele Arten technischer Produkte, angefangen beim Messer, beim Hammer oder beim Motor, können sowohl für gute wie für schlechte Zwecke genutzt werden. Niemand will Messer und Hammer verbieten, obwohl damit Menschen getötet werden können. Weil es diese Ambivalenz gibt, spricht man z.B. bei der Kontrolle des Waffenhandels von „dual use": Viele für militärische Zwecke geeignete Geräte werden in Friedenszeiten für friedliche Verwendungen eingesetzt: Lastwagen können Lebensmittel, aber eben auch Raketen befördern. Niemand denkt daran, Lastwagen zu verbieten oder ihre Nutzung aufs strengste einzuschränken, weil sie unter Umständen auch Kanonen zum Einsatzort bringen.

Was es bedeutet, wenn wir uns „vorauseilend vor Gewalten ducken, die in Zukunft einmal kommen könnten", hat besonders deutlich der Blogger Christian Heller formuliert:

> „Es verschafft vielleicht ein Sicherheitsgefühl. Aber sehr viel tatsächliche Sicherheit steckt hinter diesem Gefühl nicht. Vorauseilendes Ducken führt vor allem zu einem: dass man schon hier und heute so lebt, als wäre die Diktatur längst über uns gekommen.

127 Dazu sehr klarsichtig auch Heller 2011, S. 102 ff., 158 ff.

> Doch mit Duckmäusertum und Flucht ins Verborgene lässt sich keine Freiheit verteidigen. Gibt es eine gesellschaftliche Freiheit, dann muss sie auch laut und stolz in Anspruch genommen, immer wieder neu behauptet und ausgereizt werden. Sich zu verstecken und den Mund zu halten, das kann unter den Bedingungen von Diktatur, Diskriminierung und Intoleranz eine überlebensnotwendige Taktik sein. Aber wer es vorauseilend tut, der wartet diese Umstände nicht nur ab, der arbeitet ihnen durch seine Zurückhaltung vielleicht sogar zu."[128]

Verdatet und verkauft? Die Standardbeispiele

Als Beispiele für besonders bedenkliche Informationssammlungen werden regelmäßig zwei Fallgruppen diskutiert: die Verwendung von Kundendaten zu Werbezwecken und die polizeiliche oder nachrichtendienstliche Überwachung. Beide Themen sind freilich bei genauer Betrachtung sehr viel differenzierter zu beurteilen.

Persönlichkeitsprofile aus Kundendaten

Dass Unternehmen von ihren Kunden Daten erheben und diese dann zu Werbe- und Marketingzwecken auswerten, gilt vielen – wenn nicht der Mehrheit der Menschen – als anstößig, und zwar schon lange vor der Einführung des Internets. Man empört sich darüber, dass Handelsunternehmen sich Namen, Anschriften und Geburtstage von Kunden geben lassen und diese Daten dazu benutzen, mit individuell adressierten Sendungen für ihre Waren zu werben. Man findet es unangenehm, dass solche Unternehmen zum Zwecke der Kundenbindung Rabatt- oder andere Vergünstigungssysteme einführen und dabei weitere Angaben speichern, z.B. die Art der gekauften Waren.

Was also geschieht, wenn Unternehmen systematisch Informationen über bestimmte Personen sammeln (zum Beispiel Angaben aus Bestellungen, Zahlungsvorgängen oder dem Anklicken bestimmter Internetangebote)?[129] Sie fertigen „Persönlichkeitsprofile" an. Sie stellen aus den verschiedenen Einzelinformationen eine Art Mosaik zusammen, das die Vorlieben und Abneigungen, typische Verhaltensweisen, häufige Aufenthaltsorte und ähnliche Charakteristika der betreffenden Personen wiedergibt. Für Werbezwecke werden aus diesen „Profilen" Personen*gruppen* gebildet, die in gleicher Weise angesprochen werden. Man erarbeitet

128 Heller 2011, S. 160.
129 Zu den üblichen Verfahrensweisen s. etwa Pariser 2011 sowie Kurz/Rieger 2011, S. 13 ff..

also eine Sammlung von Namen und Adressen, an die aus bestimmten Anlässen (neue Angebote, Sonderaktionen, Umfragen usw.) mit Hilfe automatischer Drucker zahllose gleiche, aber persönlich adressierte Briefe geschrieben werden.

Sämtliche Methoden der Kundendatenauswertung beruhen auf der Grundüberlegung von Psychologen und Marketingexperten, dass jemand, der einmal oder mehrfach bestimmte Waren bestellt oder Interessen oder Vorlieben gezeigt hat, auch ein zweites oder drittes Mal gleiche oder bestimmte andere Bestellungen aufgeben werde. Diese Grundidee wird x-fach variiert; denn man nimmt an, dass Entscheidungen für die eine Ware oder die eine Dienstleistung Interesse auch für andere – teils verwandte, teils einer anderen Warenart oder Dienstleistungssparte zuzuordnende – Angebote vermuten lässt. Nonkonformistische Auswahlentscheidungen oder vorgetäuschtes Interesse kommen in diesem Kalkül nicht vor. Wenn ich mich einmal über Babywäsche informiert habe, werde ich als jemand angesehen, der sich dauernd für Strampler interessiert. Wenn ich im Internet esoterische Literatur gekauft habe, gelte ich als Liebhaber dieser Gattung. Dass es sich um einmalige Neugierde gehandelt haben kann oder dass ich jemand anders mit dieser Ware beglücken wollte, kann das System nicht erkennen. Dass man manche Druckerzeugnisse gerade deshalb erwirbt, um die Gegenposition zur eigenen Meinung kennenzulernen, ist in der Perspektive der Werbepsychologen nicht vorgesehen. Sie können derartige Abweichungen vom Mainstream nicht berücksichtigen und liegen schon deshalb oft falsch.

Das millionenfach propagierte Bild vom „gläsernen Menschen“ führt in die Irre. Die Adressaten sind nur scheinbar transparent. Durch Glas kann man hindurchblicken, die Außenhaut durchdringen, aber was sieht man als Ergebnis der Datensuche und Datenauswertung, sei sie noch so raffiniert angelegt? Jedenfalls nicht die Seele, die geheimen Regungen des Individuums! Der gläserne Mensch ist wie das vom Fleisch befreite Skelett: ein Ausstellungsstück, aber kein Individuum. Die Person, die gemeint ist, lässt sich damit nicht fassen. Die entindividualisierten Abbilder real existierender Menschen sind so wertvoll wie eben eine Adresssammlung potentieller Kunden sein kann.

Warum die Firmen dies praktizieren, ist schon gesagt worden: Sie schließen aus bisherigen Einkäufen auf künftige, hoffen auf die Wiederholung der Routinevorgänge, wollen Kunden an sich binden und neue gewinnen. Das gelingt in vielen Fällen, in anderen misslingt es. Aber in keinem Fall ist der so angesprochene Kunde „verdatet und verkauft“. Jeder ist und bleibt frei darin, die Werbesendungen in den Papierkorb zu werfen oder auf dem Computer zu löschen. Insofern besteht kein Unterschied zwischen gezielter und ungezielter Werbung. Dass die Wirtschaftswerbung mit Personendaten hierzulande seit Jahrzehnten Gegenstand einer derart intensiven und teilweise fanatischen Diskussion ist, lässt an unserem Urteilsvermögen zweifeln. In ärmeren Ländern wird man diese Diskussion für die Luxusbe-

tätigung einer Überflussgesellschaft halten und meinen, wir hätten keine anderen Probleme – in Wahrheit haben auch wir wichtigere und sollten unsere Kräfte darauf konzentrieren.

Schutz vor Belästigung – und vor wirklichen Nachteilen

Was der Papierkorb nicht leistet, ist die Abwehr unerwünschter „Anmache". Es ist in erster Linie das Recht des *Verbraucherschutzes*, das die Methoden der Kundenwerbung beschränkt: die unlautere Werbung, die unerbetenen „cold calls", die Überrumpelung der Angesprochenen am Telefon. Diese Rechtsmaterie ist in den letzten Jahren ausgebaut und verfeinert worden und schützt uns jetzt ziemlich umfassend gegen unfaire Methoden. So ist nunmehr die Werbung mit Telefonanrufen, Fax- und E-Mail-Sendungen gegenüber Verbrauchern verboten, wenn keine vorherige ausdrückliche Einwilligung des Angerufenen bzw. Adressaten vorliegt. Auch die Verwendung automatischer Anrufmaschinen gilt als „unzumutbare Belästigung".[130]

In manchen Fällen kommt hinzu, dass die verwendeten Anschriften auf fragwürdige Weise erlangt worden sind, so wenn Kundendaten ohne die erforderliche Einwilligung gespeichert und weitergegeben wurden. Diese Form der Datennutzung ist ebenfalls vor einiger Zeit strenger als zuvor geregelt worden, und das geltende Recht macht es den Adresshändlern ziemlich schwer, ihre Bestände weiter zu verwenden, zu aktualisieren und zu erweitern.[131] Andererseits ist es durchaus möglich, dass die Sammlung der Daten rechtmäßig war und sich Betroffene trotzdem mit Recht über die Art und Weise beschweren, wie ihnen Werbung geschickt wird – zum Beispiel wenn entgegen einem Aufkleber „Keine Werbung" der Briefkasten vollgestopft wird. Der Datenschutz ist also, wenn überhaupt, nur marginal und indirekt einschlägig. Er ist nicht zu dem Zweck eingeführt worden, die Papierproduktion für überflüssige Werbung zu beschränken. Den Zweck, vor Belästigungen zu schützen, erfüllt das Verbraucherschutzrecht, ohne auf die Gefühle der Betroffenen abzustellen und ohne den moralgeladenen Hintergrund des Menschenwürdeschutzes.

Das hat sich aber noch nicht überall herumgesprochen. So hat das Landgericht Lüneburg vor einiger Zeit den Absender einer Werbesendung zur Unterlassung verurteilt und dies nicht nur damit begründet, dass es sich um eine unzumutbare Belästigung handle, sondern auch dass damit in das Recht auf „informationelle

130 § 7 Abs. 2 Nr. 2 und 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) i.d.F.v. 3.3.2010, BGBl. I S. 254.
131 §§ 28, 29 BDSG i.d.F.v. 14.8.2009, BGBl. I S. 2814.

Selbstbestimmung“ eingegriffen werde.[132] Das ist eine merkwürdige Grundrechtsinterpretation: Mein angebliches Recht, selbst zu bestimmen, welche Daten über mich verwendet werden dürfen, soll als Hebel dienen, um zu verhindern, dass jemand mir unter meiner zutreffenden Anschrift etwas schickt! Nicht die Speicherung oder Weitergabe der Adresse war hier rechtswidrig, sondern (vielleicht) die Zustellung. Übrigens: Wenn der Zeitungsbericht über diese Entscheidung richtig ist, war die Werbung gar nicht adressiert, sondern es handelte sich um ein durch Boten oder durch die Post verbreitetes Anzeigenblatt. Es ging also nicht um informationelle Selbstbestimmung, sondern um den Schutz vor unbefugter Benutzung eines fremden Briefkastens.

Sieht man davon einmal ab und versucht herauszufinden, was den Betroffenen durch eine unerwünschte Benutzung ihrer Namen und Adressen angetan wird, bleibt herzlich wenig übrig. Die Unternehmen spionieren nicht hinter ihren Kunden her – täten sie dies, würden sie die gewünschte Kundenbindung selbst zunichtemachen und wären schnell allgemein in Verruf. Auch die Auswertung von Kaufgewohnheiten und Vorlieben ist keine Bosheit, mag auch mancher es bedauern, dass er immer wieder Gleiches angeboten bekommt und die Unternehmen ihm nicht einmal etwas überraschend Neues vorschlagen.

Dass die aus der allgemeinen Vernetzung entstehenden Unannehmlichkeiten auch ohne Berufung auf den Datenschutz bekämpft werden können, zeigt ein Urteil des Landgerichts Köln, das sich mit der unverlangten Zusendung von E-Mail-Werbung befasst: Zwar wurde der Unterlassungsklage eines Rechtsanwalts gegen den E-Mail-Versender stattgegeben, aber nur mit der Begründung, es handle sich um einen unzulässigen Eingriff in den „eingerichteten und ausgeübten Gewerbebetrieb“ des Anwalts; zum Datenschutz enthält dieses Urteil nichts.[133]

Wer sich schon dadurch beeinträchtigt fühlt, dass er von einer Firma mit seinem korrekten Namen angesprochen und an seine früheren Einkäufe erinnert wird, moniert im Kern, dass in der Verwendung der Daten eine Missachtung der Persönlichkeit liege. Wer nicht will, dass die beteiligten Unternehmen seine Existenz zur Kenntnis nehmen wollen, hält den Gebrauch und erst recht den Verkauf von Daten über ihn oder sie für eine Verletzung des Selbstbestimmungsrechts. Aber die werbenden Unternehmen wollen natürlich keinesfalls ihren möglichen Kunden zu nahe treten; tatsächlich erfahren sie ja gar nicht, welche konkreten Personen in ihren Werbekampagnen angesprochen werden. Die Computer, die derartige Aufträge ausführen, „wissen“ nicht, an wen die Briefe gehen, und „wollen“ gar nichts. Irgendwelche Schäden oder Nachteile materieller Art treten nicht ein, solange die Kundendaten – wie es ganz überwiegend geschieht – nur für Werbung und Marketing verwendet werden.

132 Az. 4 S 44/11, Bericht im Hamburger Abendblatt vom 6.1.2012.
133 Urteil des Landgerichts Köln v. 13.10.1998, abgedruckt bei Kröger/Hanken 2003, S. 523 ff.

Die allenthalben geäußerte Empörung über diese Praxis steht in einem befremdlichen Gegensatz zu der Selbstverständlichkeit, mit der wir von der Wirtschaft Erfolg und immer mehr Expansion erwarten. Existenzgründer sind auf Adressen potentieller Kunden angewiesen, und ein Unternehmen, das neue Kundenkreise sucht, kann nicht erst alle in Betracht kommenden Besteller fragen, ob sie überhaupt (per Post) angesprochen werden möchten (anders, wie gesagt, ist es bei der Telefonwerbung). Ich behaupte, dass die ganz überwiegende Mehrheit derer, die vor die Alternative gestellt würden, Werbung zu akzeptieren oder einen Rückgang des Wirtschaftswachstums hinzunehmen, sich für die erste Alternative entscheiden würde. So sensibel ist wohl kaum jemand, dass er die Datennutzung der werbenden Wirtschaft als schlechthin unerträgliche Kränkung seines informationellen Selbstbestimmungsanspruchs ansähe. Wer in diesem Zusammenhang behauptet, die Menschenwürde selbst sei verletzt, wenn eine Firma Namen und Anschriften regelwidrig verwendet, greift entschieden zu hoch – ich erkenne hier ein gehöriges Maß an Wichtigtuerei.

Wirkliche Nachteile entstehen jedoch aus der Verwendung von Kundendaten, wenn auf dieser Grundlage Entscheidungen zu Lasten der Kunden getroffen werden. So wird die Sammlung und Übermittlung von Daten über Zahlungsvorgänge zum Risiko für die Betroffenen, wenn daraus Aussagen über die Kreditwürdigkeit abgeleitet oder Personalentscheidungen getroffen werden sollen. Die Schufa[134], die Kreditauskunfteien und Detekteien leisten solche Dienste, und man darf vermuten, dass schon vielen Bank- und Sparkassenkunden ein Kredit verweigert worden ist, weil diese Institute negativ bewertete Angaben übermittelt haben. Aber diese Praxis ist schon lange von den Datenschutz-Aufsichtsbehörden kritisch untersucht und in vielerlei Hinsicht kritisiert worden; die Branche selbst und der Gesetzgeber haben reagiert und strengere Regeln eingeführt.[135] Das Verbot der Ableitung nachteiliger Entscheidungen aus automatisierter Datenauswertung (§ 6 a BDSG) wird leider weithin ignoriert.

Wieder anders ist die Lage natürlich, wenn Daten gestohlen und für Betrügereien verwendet werden. Selbstverständlich muss es verhindert werden, dass jemand unter fremdem Namen Bestellungen aufgibt oder kompromittierende Äußerungen versendet oder gar ins Netz stellt. Aber das ist so unbestritten wie die Geltung des Strafgesetzbuches – dass trotz des geltenden Rechts Betrug und Diebstahl vorkommen, deutet nicht auf eine Lücke im Gesetz, sondern Missachtung desselben. Der Vollzug des Datenschutzrechts ist kein politisches Thema, sondern eine Aufgabe der Aufsichtsbehörden und Gerichte – und vor allem der Bürger selbst, die

134 „Schutzvereinigung für allgemeine Kreditsicherung“, die Vereinigung der Banken und Sparkassen zum gegenseitigen Informationsaustausch über ihre Kunden.

135 So sind in der Datenschutznovelle 2009 insbesondere die Datenübermittlung an Auskunfteien (§ 28 a BDSG) und das Scoring (Einschätzung der Kreditwürdigkeit aufgrund von Datenanalysen) strenger geregelt worden (§ 28 b BDSG).

sich im täglichen Umgang mit Informationen über Dritte angemessen und fair verhalten sollen. Wenn die Betroffenen von Rechtsverstößen erfahren, können sie sich an staatliche Stellen wenden, die ihnen helfen.

Die beste Vorbeugung gegen Datenmissbrauch besteht übrigens darin, die Regeln der Daten*sicherung* ernst zu nehmen. Hier liegen die Herausforderungen für Informatiker und Techniker. Sie sind es, die ganz praktisch und konkret dafür sorgen müssen, dass die Daten auf den diversen Rechnern und im Netz wirklich sicher sind, dass sie an die richtigen Adressaten geleitet und nicht zwischendurch abgezapft werden. Die gesetzlichen Vorschriften zur Datensicherung sind einigermaßen klar (wenn auch immer noch verbesserungsbedürftig), und die untergesetzlichen Standards und Gebrauchsanleitungen müssen von der Gemeinschaft der Experten erarbeitet und durchgesetzt werden. Die Politiker können die öffentliche Verwaltung dazu nötigen, sich an diese Regeln zu halten; der Ruf nach neuen Gesetzen hilft hier gar nichts.

Das Beispiel Vorratsdatenspeicherung

Kriminalisten gehen anders an die Arbeit. Wenn sie das „Profil" eines gesuchten Straftäters zeichnen wollen, müssen sie gezielter vorgehen als die Marketingleute. Eine Gruppenbildung reicht ihnen nicht aus, sozialpsychologische Gesetzmäßigkeiten mögen ergänzend eine Rolle spielen, aber die Auswertung von Kundendaten dürfte ihnen im Zweifel kaum weiterhelfen. Für manche Straftaten ist es nützlich, Kontobewegungen Verdächtiger zu verfolgen; das ist in gewissem Rahmen zulässig, um die organisierte Kriminalität zu bekämpfen. Bei Rasterfahndungen werden nach recht groben Kriterien Gruppen gebildet, um daraus durch Abgleich mit vorhandenen Daten überhaupt erst einen Kreis von Verdächtigen herauszuarbeiten; erst *nach* diesem Auswahlprozess beginnt die kriminalistische Ermittlungsarbeit an den einzelnen Datensätzen.

Keine Datensammlung hat so viel Empörung ausgelöst wie die „Vorratsdatenspeicherung": die Speicherung der Verkehrs- oder besser Verbindungsdaten aus unseren alltäglichen Telekommunikationsbeziehungen (Telefon, E-Mail, Fax, Internetverbindungen). Wenn diese Angaben ausgewertet werden, lassen sich daraus sämtliche technisch vermittelten Kommunikationen aller Personen zusammenstellen, die sich auf dem Staatsgebiet befinden oder befunden haben. Sicherheitsbehörden können auf diese Weise herausfinden, wer mit wem in Kontakt steht oder gestanden hat, und aufgrund der Besonderheiten solcher Kommunikationsprofile (z.B. der Kommunikationspartner, der Häufigkeit und dem Ort des Gesprächs oder des Internetanschlusses) kann man weiter „kombinieren". Aus auffälligen Verhaltensweisen können kriminalistische Schlüsse gezogen werden, und vielleicht er-

geben sich aus solchen Spekulationen sogar Hinweise auf Eigenschaften einzelner Personen.

Solche Vermutungen und Schlussfolgerungen können entscheidend zur Aufklärung von Straftaten beitragen. So wäre vielleicht auch die Mordserie der Zwickauer Neonazis mit Hilfe von Telefonverbindungsdaten vor Jahren aufklärbar gewesen – wenn man diese Vorratsdaten damals gehabt und ausgewertet hätte, um das Unterstützernetz aufzuspüren und damit an die Täter heranzukommen (das liegt freilich so lange zurück, dass es keine Rolle mehr spielt, ob die Vorratsdatenspeicherung heutzutage zulässig ist oder nicht). Auch zur Abwehr von Angriffen auf Leib und Leben, seien es terroristische Attentate oder „normale" Gewalttaten, kann die Möglichkeit, die Telekommunikations-Kontakte Verdächtiger zu untersuchen oder aus den Daten Dritter auf verdächtige Kontaktpersonen zu schließen, von großem Nutzen sein.

Es liegt auf der Hand, dass eine solche Datensammlung riesige Ausmaße annimmt. Auch wenn die Daten – wie geschehen – „nur" für sechs Monate aufbewahrt werden mussten, waren die erforderlichen Speichervolumina gewaltig – ein Grund für die Telekommunikations-Unternehmen, sich heftig gegen diese Pflicht zu wehren, zumal sie dafür nicht entschädigt werden sollten. Vor allem aber wandten sich viele Bürger gegen die gesetzliche Ermächtigung zu dieser Datensammlung. Einige Prominente, darunter die spätere Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger, und ihr Parteifreund Burkhard Hirsch, erhoben in Karlsruhe Verfassungsbeschwerde, und über dreißigtausend andere schlossen sich ihnen an. Die liberalen Medien unterstützten diesen juristischen Kampf gegen eine „Errungenschaft" der Kriminalistik, die ihnen als ein gigantischer Einbruch in die Freiheit des Individuums erschien. Überall las man, die Sammlung dieser Daten ermögliche „besonders intensive Grundrechtseingriffe".

Das hohe Bundesverfassungsgericht hat daraufhin die Vorratsdatenspeicherung zwar als kriminalistisches Instrument gebilligt, aber ihre Regelung im Telekommunikationsgesetz und in der Strafprozessordnung für verfassungswidrig erklärt. Es hat einerseits betont, dass die Verbindungsdaten „für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung" sind. Auch gegen die Dauer der Speicherpflicht – sechs Monate – hatten die Richter keine Bedenken, wohl aber gegen die gesetzliche Ausgestaltung: Es fehle an „hinreichend anspruchsvollen und normenklaren Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes".[136] Deshalb verstießen die Vorschriften gegen das Fernmeldegeheimnis (Art. 10 Grundgesetz).

Die Kläger hatten argumentiert: Die Speicherung sei gar nicht geeignet, organisierte Kriminalität zu bekämpfen und terroristische Anschläge zu verhüten. Der

136 Urteil des Bundesverfassungsgerichts v. 2.3.2010, BVerfGE 125, S. 260 ff.

Eingriff in das Fernmeldegeheimnis sei deshalb so schwer, weil „alle Menschen" betroffen seien, „die Telekommunikationsdienste für die Öffentlichkeit in Anspruch nehmen". Andererseits meinten die Beschwerdeführer (mit Recht), „die Wahrscheinlichkeit, dass die gespeicherten Daten später zu Gefahrenabwehr- oder Strafverfolgungszwecken benötigt würden, sei verschwindend gering". Daraus schlossen sie aber nicht, dass die ganze Sammlung harmlos sei, sondern beriefen sich darauf, dass die Speicherung „das Risiko" erhöhe, „zu Unrecht Ermittlungsmaßnahmen ausgesetzt oder unschuldig verurteilt zu werden. Außerdem könnten solche Daten „gezielt gegen missliebige Personen eingesetzt werden". „Nur das Absehen von der Speicherung schütze wirksam vor Missbrauch".[137] – Einen besonderen Teil der Beschwerde bildet die Rüge, dass die Vorratsspeicherung „unverhältnismäßig in die Berufsfreiheit der Angehörigen von Vertrauensberufen" eingreife (und in der Tat kann die Registrierung von Kontakten zu Rechtsanwälten, Steuerberatern, Seelsorgern, sozialen und psychologischen Beratern und Investigativ-Journalisten besonders heikel sein).

Das Gericht hat sich auf die Vermutungen und Befürchtungen der Beschwerdeführer weitgehend eingelassen. Der Kern des Urteils ist eine Aussage, die neue Methode der Datensammlung verursache bei den Bürgern einen Einschüchterungseffekt, ein „diffus bedrohliches Gefühl des Beobachtetseins", also die Angst vor einer unheimlichen, nicht abzuwehrenden Macht, die ihnen etwas Verbotenes oder Unerwünschtes vorhalten und ihnen deswegen ein Übel antun will. Dieses Gefühl könne „eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen".[138] Das ist keine empirisch begründete Feststellung, sondern eine Vermutung der Richter, und sie soll als Begründung dafür dienen, dass die Speicherung nur unter strengen Voraussetzungen erlaubt sein darf. Genau genommen, ist schon dies ein Fehlschluss; denn es ist doch fraglich, ob die diffusen Ängste verschwänden, wenn der Gesetzgeber eine strengere Regelung beschlösse – was er ja nach dem Urteil darf und was überdies von der EU-Kommission angemahnt wird. Mag das künftige Gesetz auch noch so „anspruchsvolle" Voraussetzungen für die Nutzung der gesammelten Daten aufstellen und mag es noch so „normenklar" formuliert sein – der Eindruck, dass das Telekommunikationsverhalten des ganzen Volkes registriert werde, wird bleiben, und demgemäß werden auch die Proteste anhalten. Nicht zufällig fordern die Kritiker die Aufhebung der EU-Richtlinie, auf die sich die Bundesregierung beruft, und weisen darauf hin, dass auch in anderen EU-Mitgliedstaaten verfassungsrechtliche Bedenken gegen die Richtlinie

137 Ebd. S. 282 f.

138 Ebd. S. 320. An anderer Stelle des Urteils (S. 332) wird hervorgehoben, die Befugnisse der geheimen Nachrichtendienste, die TK-Daten zu verwenden, beförderten „das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise" und entfalteten „nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung".

erhoben worden sind (und einige Verfassungsgerichte diesen Bedenken gefolgt sind).

Kritik des Vorratsdaten-Urteils

Das Karlsruher Urteil wird von allen Bürgerrechtlern und ihren Verbündeten aufs höchste gelobt – und ist doch in einem zentralen Punkt höchst anfechtbar.[139] Es erklärt nämlich nicht, die Ängste der Bürger seien unbegründet. Da man somit annehmen muss, dass das Gericht diese Ängste teilt, hätte man Ausführungen darüber erwarten dürfen, wie es denn geschehen könne, dass die Daten missbraucht werden, und dass ein hohes Maß an *Wahrscheinlichkeit* dafür spreche. Mit großer Sorgfalt wird stattdessen ausgemalt, welche „Rückschlüsse" „bis in die Intimsphäre hinein" sich „bei umfassender und automatisierter Auswertung" aus den TK-Verkehrsdaten ziehen lassen. Das Misstrauen wird besonders auf die vielen privaten Anbieter gelenkt, die zur Speicherung der Daten verpflichtet sein sollten.[140] Die „Vorkehrungen", die das Gericht zur Abwehr der Risiken fordert, richten sich aber auch gegen die Behörden, die im Falle des Datenabrufs mit der Auswertung befasst sind. Ihnen wird mehr oder weniger deutlich unterstellt, dass sie regelmäßig ihre Befugnisse extrem weit auslegen, wenn nicht überziehen wollen. Weil der Schutz der Individualinteressen in verschiedenen Aspekten zu schwach ausgestaltet sei, verstoße das Gesetz gegen das Prinzip der *Verhältnismäßigkeit*. Dass dieses Prinzip auch bei der *Anwendung* des Gesetzes zu beachten ist und im Allgemeinen beachtet wird, sagen die Richter nicht. Sie vertrauen auf die Klarstellung durch den Gesetzgeber und misstrauen den Beamten.

Die schärfste Kritik an diesem Urteil ist aus dem entscheidenden Senat selbst gekommen. Die Richter *Wilhelm Schluckebier* und *Michael Eichberger* haben Abweichende Meinungen zu Protokoll gegeben, in denen sie die Vorratsdatenspeicherung für verfassungskonform erklären.[141] Der Richter Schluckebier schreibt, wenn das angemessene Niveau der *Datensicherheit* gewährleistet sei, fehle „jede objektivierbare Grundlage für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts".[142] Die Regelungen seien hinreichend angemessen und zumutbar. „Der Bürger muss sich im Rechtsstaat auf effektiven Schutz *durch* den Staat ebenso verlassen können wie auf den Schutz *gegen* den Staat".[143]

Der Richter Eichberger hat noch einen speziellen Einwand gegen die Mehrheitsentscheidung formuliert, der auch für die öffentliche Diskussion des Themas

139 Nachweise von Zustimmung und Kritik in der Lit. bei Bull 2011 a, S. 96 Fn. 220.
140 Ebd. S. 319 f.
141 Ebd. S. 364 ff. und S. 380 ff.
142 Ebd. S. 366.
143 Ebd. S. 369.

wichtig wäre: Die Senatsmehrheit ist davon ausgegangen, dass die Behörden beim Abruf der Daten stets ein umfassendes Bewegungs- und Persönlichkeitsprofil anstreben; tatsächlich aber untersuchen sie vielfach nur „einzelne Ereignisse, kurze Zeiträume und die Telekommunikationsbeziehungen nur einer oder weniger Personen (etwa die Telekommunikationsverbindungen einer Person an einem Tag oder auch nur in einer bestimmten Stunde)"; diese Abrufe haben „ein nur geringes Eingriffsgewicht" und sind schon gar nicht mit dem Zugriff auf *Inhalte* der Kommunikation vergleichbar.[144]

Je öfter ich mich in dieses Urteil und sein mediales Umfeld vertiefe und die Argumente überdenke, desto klarer wird mir, dass die Opposition gegen die Vorratsdatenspeicherung im Kern keine verfassungsrechtliche, sondern eine sozialpsychologische und politische Aktion ist. Die Bedenken, die aus dem Grundgesetz hergeleitet werden, sind ausräumbar, die in den Köpfen herrschenden Vorstellungen nicht – oder nur unter sehr günstigen Voraussetzungen. Es ist wie seinerzeit bei der Volkszählung, als die Boykottbewegung alle rechtlichen und empirisch-praktischen Argumente vom Tisch fegte: Die Volkszählungsgegner und -verweigerer wollten „der Politik" und „dem Staat" eine Lektion erteilen, und die bevorstehende Volkszählung bildete einen passenden Gegenstand. Dass die Informationen, die bei dem Zensus erhoben werden sollten, und die im Gesetz zugelassene Nutzung nicht den „Überwachungsstaat" herbeiführen würden, war vermutlich vielen Opponenten durchaus klar, aber sie fanden in dem Boykott einen Aufhänger, ihr tiefes Unbehagen über frühere Praktiken der Behörden (wie den – damals längst aufgehobenen – Radikalenerlass) und eine allgemeine Unzufriedenheit mit der Politik auszudrücken.

Die Vorstellung, dass alle unsere TK-Verkehrsdaten für ein halbes Jahr aufbewahrt und ausgewertet werden können, beunruhigt nicht nur die Mitmenschen, die etwas Verbotenes oder gar Strafbares tun wollen, sondern auch viele gesetzestreue Bürger, weil sie glauben, nicht mehr unbefangen telefonieren, faxen und mailen zu können. Dass daraus tatsächlich Ängste entstehen – und zwar gerade auch bei den „braven" Mitbürgern –, ist wahrscheinlich. An die hohen rechtlichen Hürden, die der Verwertung der gespeicherten Daten entgegenstehen, denken viele nicht, und wenn sie daran denken, sind sie sich nicht sicher, ob die Vorschriften wirklich eingehalten werden.

So spitzt sich das Problem auf die *Vertrauensfrage* zu, und es ist offensichtlich, dass Teile des Volkes und speziell große Teile der meinungsbildenden Schicht den Behörden eben nicht vertrauen. Ohne ein Mindestmaß an Vertrauen ist aber kein Staat aufrecht zu erhalten.

144 Ebd. S. 383.

Die Politik kann nicht warten, bis alle Ängste abgebaut sind. Sie muss entscheiden, ob Instrumente wie die Speicherung der TK-Verbindungsdaten wieder zulässig sein sollen oder nicht. Die Innenpolitiker, die überwiegend dazu neigen, die Arbeit der Polizeibehörden (und in engeren Grenzen auch die der Nachrichtendienste) zu erleichtern, liegen darüber im Streit mit Rechtspolitikern (der eigenen oder einer anderen Partei). Die Bundesministerin der Justiz beharrt darauf, dass allenfalls bei konkretem Anlass (wegen eines bestimmten Tatverdachts) ein „Einfrieren" der dann gerade vorhandenen Verbindungsdaten zugelassen sein sollte. Dieses Verfahren des „quick freezing" kann aber die längerfristige Vorratsdatenspeicherung nicht ersetzen; es schafft, wie auch das Bundesverfassungsgericht bestätigt hat, keine „vergleichbar effektive Aufklärungsmöglichkeit".[145] Kompromisse sind bei der Speicherungsdauer und der Eingrenzung der Zugriffsbefugnisse möglich, und hier spielt die EU-Richtlinie eine Rolle, die eine Mindestspeicherung von sechs Monaten vorschreibt.

Ein neues Szenario: Die Überwachungsmaschine

Die Entwicklung geht natürlich weiter, und so berichtet die Presse, dass derzeit – mit Unterstützung der EU – ein umfassendes Kontrollsystem entwickelt werde, dessen Überwachungskapazität alles bisher Dagewesene überschreite: „Die Überwachungsmaschine" schlechthin.[146] Unter dem Titel „Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung" (englische Abkürzung: „Indect") sollten „verschiedene Überwachungsmittel wie Kameras, Drohnen, Gesichtserkennung und Bildanalyse" zusammengeschaltet werden, ebenso wie „Webseiten, Diskussionsforen, Usenet-Gruppen, Dateiserver, Netzwerke und individuelle Computersysteme". Das Ziel sei, auf diese Weise „abnormes Verhalten" frühzeitig zu erkennen.

Ein Mitglied der Piratenpartei nennt Indect nach dem Zeitungsbericht eine „Gedankenpolizei". Über die entsprechend von Orwell erdachte Behörde hinaus brauche diese künftige Gedankenpolizei aber niemanden mehr, der auf den Bildschirm starrt; „die Maschine kann alle Bürger zu jedem Zeitpunkt erfassen". Eine schaurige Vorstellung: Der „allwissende künstliche Polizist" hat technische Augen und Ohren, kann sich Gesichter einprägen und wiedererkennen und aus dem Internet Zusammenhänge und Beziehungen zwischen weit entfernt voneinander existierenden Menschen und Organisationen aufdecken – alles mit der Intention, „abnormales Verhalten" aufzudecken und daraus polizeiliche oder justizielle Maßnahmen abzuleiten.

145 Ebd. S. 318.
146 Behrens 2011.

Diese Geschichte von der Überwachungsmaschine ist ein aktuelles Beispiel einer altbekannten negativen Utopie. Sie ist die Vorstellung einer technischen Erfindung und gleichzeitig ihre publizistische Verwandlung in eine angebliche soziale Möglichkeit, die dann eine Bedrohung für potentiell alle Menschen darstellt, die auf der Welt leben. Keine Frage: Wenn eines Tages Maschinen in Gebrauch kämen, die aus bestimmten Äußerungen, Bewegungen oder Geräuschen auf „abweichendes" Verhalten schließen und damit automatisch die gezielte Überwachung von Personen auslösen oder sogar zu physischen Freiheitsbeschränkungen führen, wäre das nicht hinnehmbar. Es wäre eine verfassungswidrige Einengung des normalen menschlichen Verhaltens, auf diese Weise Verdachtsmomente zu konstruieren, und wenn dies noch mit Hilfe von Gesichtserkennung perfektioniert würde oder zusätzliche Informationen aus dem Netz hinzugefügt würden, wäre das wirklich ein Horrorszenario. Entscheidungen dürfen überhaupt nicht allein aufgrund automatisierter Datenverarbeitung getroffen werden;[147] es muss immer ein menschlicher Entscheidungsakt hinzukommen.

Angenommen, ein derart superperfektes System werde gleichwohl hergestellt – dann hinge es von dem konkreten Zustand des Rechtsstaates, vom Rechtsbewusstsein des Volkes und der Medien und von der Rechtstreue der Regierungen und Verwaltungen ab, ob ein solches System zur Entdeckung und Bekämpfung von Alltagsstraftaten oder gar zur allgemeinen „Gesinnungspolizei" eingeführt würde. Polizei und Nachrichtendienste sind zwar an der Forschung auf diesem Gebiet interessiert, und man kann nicht ausschließen, dass sie zur Bekämpfung schwerer Straftaten und zur Abwehr schwerer Gefahren für die öffentliche Sicherheit auch extreme Mittel anwenden möchten. Aber der Gesetzgeber wird auf die rechtliche Eingrenzung solcher Systeme achten, und die Öffentlichkeit wird ihn daran erinnern. Die hohe Summe staatlicher und privater Mittel, die in die Förderung solcher Projekte fließen, lässt erahnen, dass es auch außerhalb des staatlichen Sicherheitsapparates viele Interessenten geben wird, die sich Vorteile von der technisch intensivierten Überwachung versprechen. Sicherheitstechnik ist ein explodierender Markt, der seinerseits überwacht werden muss.

Der Computer als Privatsphäre

Sehr tief geht der Eingriff der Staatsgewalt auch dann, wenn Polizei oder Verfassungsschutz über das Netz heimlich gezielt in privat genutzte Computer eindringen und Speicherinhalte „absaugen", um Verbrechen aufzuklären oder ihnen vorzubeugen. Eben das ist seit einiger Zeit möglich und unter engen Voraussetzungen

147 Vgl. § 6 a Bundesdatenschutzgesetz, der seine Entsprechung z.B. im französischen Datenschutzgesetz von 1978 hat.

gesetzlich erlaubt. So senden inzwischen die dazu ermächtigten Behörden Viren, Würmer oder „Trojaner“ auf die PCs von Verdächtigen und „durchsuchen“ sie mittels dieser Eindringlinge. Damit wird die seit längerem praktizierte Telekommunikationsüberwachung (Abhören von Telefonen, Mitlesen von Faxschreiben oder E-Mails) ergänzt; denn die Inhalte können auf diese Weise gelesen werden, bevor sie für den Transport verschlüsselt werden.

Das Bundesverfassungsgericht ist auch zu dieser Frage angerufen worden und hat festgestellt, dass eine solche „heimliche Infiltration eines informationstechnischen Systems“ zulässig ist, „wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“.[148] Das Gericht hat noch eine ganze Reihe von Vorbehalten formuliert, insbesondere dass nur ein Richter die „Online-Durchsuchung“ anordnen darf und dass der „Kernbereich privater Lebensgestaltung zu schützen“ ist. Es hat das Ganze unter die Überschrift gestellt, dass es ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ gebe.[149] Die Öffentlichkeit hat mit viel Zustimmung zur Kenntnis genommen, dass hier aus dem allgemeinen Persönlichkeitsrecht ein vermeintlich neues Grundrecht herausgelesen worden ist, und hat es begrüßt, dass die gesetzliche Vorschrift, auf die sich die Praxis gestützt hatte,[150] für verfassungswidrig erklärt wurde. Aber der Streit geht weiter, weil auch andere Rechtsnormen diese Maßnahme erlauben;[151] das Verfassungsgericht wird sich mit dieser Frage noch einmal befassen müssen.

Erstaunlich ist, dass Medien und liberale Öffentlichkeit diese Entscheidung des obersten Gerichts fast kritiklos hingenommen haben. Immerhin wird darin zugelassen, dass ein Computer schon dann heimlich infiltriert wird, „wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen“. Auf die Voraussetzung, dass eine „konkrete Gefahr“ bestehen muss, wird hier also – aus guten Gründen – verzichtet, sondern es soll die „Gefahrengefahr“ genügen. Anders als bei Rasterfahndungen und der umstrittenen Vorratsdatenspeicherung dringt der Staat hier gezielt in einen Bereich ein, den jeder für sich behalten und nicht fremden Blicken öffnen will.

Muss nicht der eigene PC, der alle privaten Notizen und Kommunikationsinhalte enthält, ebenso gegen Durchsuchungen geschützt werden wie der räumliche Rückzugsbereich, die Wohnung? Wenn man dieser Überlegung folgt, ist die Heimlich-

148 BVerfGE 120, 274.
149 Nachweise zu Erläuterungen und Kritik in der Lit.: Bull 2011 a, S. 35 Fn. 86.
150 Es handelte sich um das Verfassungsschutzgesetz Nordrhein-Westfalen (dort § 5 Abs. 2 Nr. 11).
151 So das Gesetz über das Bundeskriminalamt (§ 20 k). Es ist insofern ebenfalls verfassungsrechtlich umstritten.

keit der Durchsuchung nicht hinnehmbar und letztlich in jedem Fall verfassungswidrig. Wir verlangen auch in manchen anderen Konstellationen, dass der Staat auf „an sich" verfügbare Informationen verzichtet, etwa wenn Angehörigen eines Verdächtigen oder bestimmten Berufen ein Zeugnisverweigerungsrecht zugebilligt wird.

Kriminalität und Missbrauch im Internet

Während die Datenschutz-Szene ausgiebig über die Möglichkeiten der Unterdrückung durch den Staat diskutiert, geschehen in der Praxis der Internetnutzung unglaubliche Dinge. Das Netz wird ständig dazu benutzt, anderen Schaden zuzufügen. Es beginnt beim Mobbing und Stalking über E-Mails und soziale Netzwerke, bei Beschimpfungen und Verleumdungen übelster Art und geht bis zu millionenfachem Betrug und zu anonymen Morddrohungen „aus dem Nichts". Täglich können wir Berichte darüber in den Zeitungen lesen; die Polizei veröffentlicht von Zeit zu Zeit zusammenfassende Berichte mit erschreckenden Zahlen. „Cyberbullying" und „Cyberharassment" verursachen Tragödien: Eine ganze Reihe von Schülerinnen und Schülern, die im Netz gemobbt wurden, haben sich das Leben genommen.[152] Offensichtlich äußern manche Menschen unter dem Schutz der Anonymität im Netz Dinge, die sie von Angesicht zu Angesicht nicht sagen würden, und es ist außerordentlich schwer, ihnen das zu verwehren. Manche sind allerdings frech genug, sich für „Hassreden" auf die Meinungsfreiheit zu berufen; „free speech" ist zumindest in der amerikanischen Diskussion über verletzende Äußerungen ein vielbenutzter Rechtfertigungstopos.

Auch der materielle Schaden durch Internetstraftaten ist vermutlich riesig. Es ist vorgekommen, dass prosperierende Unternehmen durch ungetreue Mitarbeiter oder Eindringlinge von außen, die das Computersystem oder den E-Mail-Zugang manipulierten, in den Konkurs getrieben wurden. Einige Hacker halten sich viel darauf zugute, dass sie fremde Systeme stören oder gar zerstören können. Ganze Industriebetriebe wurden durch eingeschleuste Viren, Trojaner oder wie immer die Schadprogramme heißen, lahmgelegt – und vieles mehr.

Dass Computerkriminalität der verschiedenen Arten bekämpft und bestraft werden sollte, ist eigentlich nicht umstritten, aber die Täter profitieren davon, dass Teile der Netzgemeinde jegliche staatliche Kontrolle im Netz ablehnen – sie denken nur an ihre eigene (gesetzeskonforme) Nutzung der Online-Welt und fürchten, die Behörden würden ihre Überwachungsbefugnisse auch gegen die „braven" Netzfreaks richten. In der Tat werden natürlich bei Durchsuchungen immer auch Un-

152 Vgl. etwa Plotkin 2012, S. 2 ff.

schuldige überprüft (da man die Schuldigen noch nicht kennt, ist dies selbstverständlich!) – aber auch dies ist in der realen Welt nicht anders, und wenn gewisse Grenzen eingehalten werden, muss jeder dies ertragen.

Zu diesen Grenzen gehört vor allem die Unschuldsvermutung, und besonders besorgte Netznutzer meinen, wenn die Polizei zu ermitteln anfange, halte sie jeden und jede für verdächtig. Die These von dem „Generalverdacht", der z.B. allen Rasterfahndungen zugrunde liege, ist irgendwann einmal als Argument gegen solche Massenaktionen der Sicherheitsbehörden aufgestellt worden; sie war nie wirklich begründet, aber sie hält sich hartnäckig. Wie aber soll denn eine Behörde auf die Täter kommen, wenn sie nicht stufenweise die möglichen Verdächtigen feststellen und den Kreis der potentiell Verantwortlichen immer weiter einengen darf? Es muss nur sichergestellt sein – und das ist regelmäßig der Fall, jedenfalls in Deutschland –, dass die Daten über die große Zahl der danach nicht Verdächtigen wieder gelöscht werden.

Zweiter Teil: Die ökonomische und technische Perspektive

Für Wirtschaft und Technik stellt sich manches ganz anders dar als für Staat und Politik. Während die öffentliche Verwaltung an Recht und Gesetz gebunden ist, ja ohne gesetzliche Grundlage gar nicht eingreifend tätig werden darf, sind unternehmerische Initiative und richtiger Einsatz der Technik die wichtigsten Faktoren wirtschaftlichen Erfolges; wer etwas unternimmt, nutzt seine Freiheit und darf darin nur beschränkt werden, wenn dies verfassungsrechtlich zugelassen ist. Das Internet zu nutzen ist in dieser Perspektive ebenfalls ein Akt der Freiheit, aber das Recht ist auch hier im Spiel – als die Instanz, die Handlungsräume eröffnet und gleichzeitig Grenzen zieht.

Geschäftsmodelle und Risiken

Die Internetwirtschaft boomt. Das Netz und seine Umgebung sind für Unternehmer eine Goldgrube. Allein der ständige Ausbau und die Unterhaltung des Netzes erfordern große Investitionen und bieten Renditechancen. In besonders großem Maßstab wird an den angeschlossenen Geräten und den notwendigen Programmen verdient. Von dem gewaltigen Stromverbrauch für das Internet und die daran teilhabenden Computer wird zwar selten gesprochen; es liegt auf der Hand, dass auch dieser Aufwand die Wirtschaftsleistung der beteiligten Länder erhöht. Dass im Netz und um das Netz herum unzählige Kauf- und Dienstleistungsangebote platziert werden, bedeutet eine riesige Ausdehnung der Märkte.

Informationen werden bisher vielfach unentgeltlich angeboten, aber die Netzbetreiber lassen sich die entsprechende Werbung von den Anbietern bezahlen. Die Nutzer wiederum „zahlen" – meist ohne sich das klarzumachen – mit ihren persönlichen Angaben; die Daten sind im Internet eine wertvolle „Währung".[153] Vielen halten diesen „freien" Markt für den Normalzustand und die Entgeltlichkeit von Medienangeboten für die unerwünschte Ausnahme – aber das widerspricht der Logik der Wirtschaft. Nur solange die Kosten der Webseiten durch die Werbeeinnahmen überkompensiert werden, kann es bei der Unentgeltlichkeit bleiben; diese Zeiten werden vielleicht schon bald vorbei sein.

Niemand weiß, welche Firmen dauerhaft Gewinne bringen werden. In den wenigen Jahren, seit es das Internet gibt, sind bereits einige Unternehmen abgestürzt, waren plötzlich nur noch einen Bruchteil dessen wert, was die Börse, die Rating-

153 Zu diesem Tatbestand s. u. a. Kurz/Rieger 2012, S. 13 ff.

agenturen oder die Fachpresse ihnen attestiert hatte; viele, die mit großen Erwartungen gestartet waren, sind nach einiger Zeit wieder ganz von der Oberfläche verschwunden. In keinem anderen Wirtschaftszweig waren die „Blasen" so groß und sind so spektakulär geplatzt wie in der Informations-, Medien- und Kommunikationswirtschaft. Die „sozialen Netzwerke" wie Facebook und Twitter leben von aktuellen sozialen Moden. Sie sprechen vor allem die Jugend an (und in ihrem Gefolge alle möglichen Institutionen und Unternehmen, die sich unter dem Titel „Freunde" neue Kunden oder Sympathisanten beschaffen wollen). Wenn die jugendlichen Facebook-Enthusiasten sich an die neuen „Freundeskreise" gewöhnt haben, finden sie es vielleicht bald gar nicht mehr „cool", sondern langweilig, ständig dort zu kommunizieren. Sie werden älter und wollen vielleicht von all dem schönen Zauber gar nichts mehr wissen. Dann kann es sehr schnell mit den Teilnehmerzahlen abwärts gehen. Sind die Unternehmen dann hoch verschuldet oder leisten sie sich Managementfehler, ist ihre Existenz gefährdet. Andere Unternehmen werden auf ihren Spuren wandeln und versuchen, die Märkte auszuschöpfen, aber möglich ist auch eine allgemeine Erschöpfung der Internet-Beziehungen und eine Rückkehr zu anderen Formen sozialen Kontakts. Die vorübergehende Schwäche der Facebook-Aktien an den Börsen war ein Warnsignal: Die Bäume wachsen nicht in den Himmel.

Kurz gesagt, ist die Lage der Internetwirtschaft nicht besser und nicht schlechter als die anderer Wirtschaftszweige – nur dass die finanziellen Volumina, um die es geht, oft erheblich größer und die Entwicklungsaussichten ungewisser sind. Die Online-Wirtschaft kann in kurzer Zeit mit relativ geringem Aufwand so große Mengen von Individuen als Kunden gewinnen wie kein anderer Wirtschaftszweig; daher sind die Gewinnchancen so groß wie kaum irgendwo sonst. Ähnlich groß ist aber auch das Verlustrisiko. Im Kern aber gilt: Ob online oder offline, die Entwicklung eines Unternehmens hängt mehr von den Geschäftsideen und den Personen an der Spitze ab als von der technischen oder nicht-technischen Vermittlung der Angebote.

In der Netzwirtschaft hat sich ursprünglich eine Gruppe klarsichtiger junger Leute durchgesetzt, die frühzeitig das enorme wirtschaftliche Entwicklungspotential technischer Geräte und technisch vermittelter Leistungen erkannten und die den Mut hatten, mit wenig Eigengeld und viel Schulden, aber auch mit großer Disziplin und persönlichem Einsatz unternehmerisch anzufangen. Sie trafen den Geist der Zeit, und da „nichts erfolgreicher ist als der Erfolg", sind sie von Beobachtern und Begleitern immer höher gejubelt und geschrieben worden. Je mehr Menschen sich Computer kaufen und im Netz surfen, desto glänzender strahlt der Ruhm der Erfinder und Manager. Um Ruhm und Größe aber rankt sich Geheimnis, Kritik verstummt, Phantasie blüht.

Erwartbar war auch, dass die Ausdehnung der Internetwirtschaft einige bisher erfolgreiche Geschäftsmodelle in Bedrängnis gebracht hat. Wenn sehr viele Menschen sich im Internet orientieren, dort Bestellungen aufgeben und sich Musik anhören und Videos ansehen, gehen die Umsätze der traditionellen Medien, des Buchhandels und der Platten- und Filmhersteller zurück. „Einige der wichtigsten Sub- und Popkulturphänomene" sind heute im Netz zu finden[154]. Die bisher auf diesen Märkten etablierten Unternehmen müssen sich umstellen: Die Hersteller von Lexika bedienen die Leserschaft ebenso über das Netz wie die Zeitungen und Fernsehanstalten ihr elektronisches Angebot durch online-Angebote ergänzen.

Der Streit um das Urheberrecht: Das Ob und das Wie

Die Gewöhnung an Unentgeltlichkeit

Viele meinen nun, dass auch die Nutzung des Netzes und der dort angebotenen Informationen und Kommunikationsmöglichkeiten für jedermann unentgeltlich sein müsse. Das ist aber alles andere als selbstverständlich. Unser Wirtschaftssystem beruht vielmehr darauf, dass jede Leistung – zumindest jede individuell zurechenbare Leistung – eine Gegenleistung verlangt. Nur ausnahmsweise erbringt die Allgemeinheit die Gegenleistung oder der Leistende finanziert sie auf andere Weise, im Netz vornehmlich durch Einnahmen aus der Werbung und der Auswertung von Kundendaten. Die Theorie der „Allmende", also der genossenschaftlichen Nutzung von Gemeingütern unabhängig von Marktmechanismen,[155] findet zwar neuerdings unter Netzexperten Aufmerksamkeit, bleibt in der Praxis der Wirtschaft aber bislang ohne Wirkung.

Die Erwartung der meisten Nutzer, dass im Netz kostenlos zu haben sein müsse, was offline seinen Preis hat, beruht offensichtlich auf Gewohnheit, nämlich auf der Erfahrung, dass eben dies bisher möglich ist. Ist aber dadurch schon Gewohnheitsrecht entstanden? Wir sind durch die unentgeltliche Präsentation der Inhalte von Zeitungen und Zeitschriften und durch das Herunterladen aller möglichen Programme verwöhnt, ohne viel darüber nachzudenken, wie denn die Kosten des Netzes aufgebracht werden.[156] Viele finden es auch ganz in Ordnung, dass sie Musik und Filme, die sie sonst kaufen oder gegen Entgelt ausleihen müssten, „umsonst" aus dem Netz beziehen – womit meist Urheber- und Leistungsschutzrechte der Autoren, Komponisten und darbietenden Künstler verletzt werden. Seit einiger Zeit lassen die Rechteinhaber solche illegalen Nutzungen durch Verwertungsgesell-

154 Kreye 2011.
155 Vgl. Ostrom 1999.
156 Wie hoch diese sind, haben u.a. Kurz/Rieger 2012, S. 14 ff. anschaulich beschrieben.

schaften oder Anwälte systematisch verfolgen, kassieren zunehmend Entgelte und verlangen – mit Erfolg – auch Erstattung der Gebühren für diese Rechtsdurchsetzung; einige Anwaltsbüros verdienen prächtig an dem formularmäßigen Einzug dieser Gelder.[157] Durch Fehler bei der IP-Feststellung werden dabei offenbar immer wieder auch die Falschen herangezogen, und angesichts der allgemeinen Technikgläubigkeit fällt es ihnen schwer zu beweisen, dass sie die betreffenden Inhalte gerade nicht heruntergeladen haben.

Kein Wunder, dass die ertappten Sünder und eben auch rechtmäßige Internetnutzer die „Freiheit des Internet" beschwören; niemand lässt sich gern rechtswidriges Handeln vorwerfen, und niemand zahlt gern die Kosten seiner eigenen Demütigung. Zur Entschuldigung der Urheberrechtsverletzer mag es auch beitragen, dass viele Internet-Anbieter in der Vergangenheit eben nicht auf Entgelten bestanden haben, sondern die kostenlosen Angebote als verlockende Kostproben ihrer Produktion, also zu Werbezwecken ins Netz gestellt haben.

Dass das Surfen im Netz frei sein soll, folgt – wie ausgeführt – aus der grundrechtlichen Informationsfreiheit gemäß Art. 5 Abs. 1 Satz 1, Halbsatz 2 GG: Das Netz ist eine „allgemein zugängliche" Informationsquelle. Aber das Grundrecht garantiert nicht die unentgeltliche Teilhabe an dem im Netz gespeicherten Wissen. Den Anbietern steht es frei, ein Entgelt zu verlangen: Dass eine Zeitung am Kiosk ihren Preis hat, stört niemanden – dasselbe Produkt, der leichteren Zugänglichkeit halber ins Netz gestellt, braucht nicht verschenkt zu werden. Der Markt verlangt möglicherweise andere Modalitäten der Bezahlung, aber er lässt sich nicht zum Verschenken von Leistungen verleiten, und der Gesetzgeber oder die Gerichte haben keinen Anlass, die Unentgeltlichkeit zu erzwingen.

Der Kampf um die Rechtspositionen

Der Streit um das Urheberrecht wird gegenwärtig weltweit ausgetragen. In den USA hat man sich insbesondere über zwei Gesetze gestritten, die der Internet-„Piraterie" entgegenwirken sollen: der Stop Online Privacy Act, kurz *Sopa* genannt, und der Protect IP Act, *Pipa*. Darin ist u.a. vorgesehen, dass Seiten aus den Suchmaschinen genommen und IP-Adressen gestrichen werden. Die Internet-Firmen wie Google, Facebook, Twitter und YouTube „laufen Sturm" gegen diese Initiativen.[158] Sie rufen „Zensur" und behaupten, die Meinungsfreiheit der Intenetnutzer zu verteidigen. Auf der anderen Seite aber kämpfen die großen Medienunternehmen wie Time Warner, Sony und CBS für die Rechteinhaber und ihre eigenen Vermarktungsinteressen, dazu die Lobbyorganisation der amerikanischen

157 Krit. dazu mit Grund u.a. Kurz 2012.
158 Klüver 2012.

Filmwirtschaft, die US-Handelskammer und der Gewerkschafts-Dachverband AFL-CIO, die ebenso wie ihre Gegenspieler um ihre Geschäfte und die Arbeitsplätze bangen. Es bleibt nicht mehr verborgen, „dass hinter den Anti-Zensur-Parolen handfeste wirtschaftliche Interesse stehen".[159]

Internet-Aktivisten haben auch in Deutschland mit großem Aufwand und scharfen Worten erfolgreich die Ratifikation des multilateralen *Anti-Counterfeiting Trade Agreement (ACTA)* bekämpft, durch das neue internationale Standards für die Abwehr von Produktpiraterie und Urheberrechtsverletzungen verbindlich werden sollten.[160] Dieses „Anti-Piraterie-Abkommen" hatten die USA, Kanada, Japan, Australien, Neuseeland, Südkorea, die Schweiz sowie die Europäische Union und die meisten ihrer Mitgliedstaaten ausgehandelt. Die Staaten sollten danach auf diesem Feld effektiver kooperieren, und sie sollten ausdrücklich verpflichtet sein, die Rechte der Urheber durchzusetzen. Gegen einige der Maßnahmen, die in dem Abkommen als „geeignet" bezeichnet wurden, richteten sich wütende Proteste, vor allem gegen Netzsperren und dagegen, dass Internet-Dienstleister auch für inhaltlich rechtswidrige Internet-Veröffentlichungen verantwortlich sein sollen.[161] Ihre rabiaten Methoden (wie die Hackerangriffe auf Webseiten der Regierungen und anderer ACTA-Befürworter) versuchte die „Web-Guerilla" damit zu rechtfertigen, dass die Verhandlungen lange geheim geführt worden sind und dass keine Vertreter der Internetnutzer hinzugezogen worden seien[162] – fast so als ob die Interessenten ein eigenes Volk bildeten, mit dem die staatlichen und internationalen Instanzen auf gleicher Ebene verhandeln müssten.

Nachdem nun auch die amerikanische Justiz gegen die Datentransferbörse *Megaupload* vorgegangen ist, die ihre Nutzer für die Bereitstellung rechtswidriger Kopien belohnte, haben Hacker der Gruppe „Anonymous" in einem angekündigten „Rachefeldzug" vorübergehend die Webseiten des FBI und des US-Justizministeriums lahmgelegt.[163] Tauschplattformen sind für ihre Betreiber offensichtlich ein gutes Geschäft; darum wird mit harten Bandagen gefochten.

Die Kritiker haben sich auf die höchsten Normen der ungeschriebenen oder geschriebenen Weltrechtsordnung berufen. So hat amnesty international behauptet, ACTA sei „eine Büchse der Pandora für mögliche Menschenrechtsverletzungen"; es habe „negative Auswirkungen auf mehrere Menschenrechte, insbesondere das Recht auf ein angemessenes Verfahren, das Recht auf Achtung des Privatlebens, die Informationsfreiheit, Meinungsfreiheit und das Recht auf Zugang zu lebens-

159 Koch 2012.
160 Text: Rat der Europäischen Union, Dokument 12196/3/11 REV 3 (de), im Internet leicht zugänglich.
161 Vgl. nur Brill 2012.
162 Brill aaO.
163 Koch/Brinkmann 2012.

wichtigen Medikamenten“[164], und wikipedia überschreibt den entsprechenden Abschnitt seines ACTA-Beitrags mit „Aushebelung der Menschenrechte und des Rechtsstaates“ – als ob das eine Tatsache wäre. Wenn das zuträfe, könnte man sich einen größeren Skandal kaum vorstellen – das Abkommen hätte dann gleiches Gewicht und wäre ungefähr ebenso verwerflich wie die Aufhebung der UN-Menschenrechts-Erklärung oder die weltweite Abschaffung der Pressefreiheit. Erstaunlich, dass solch eine offensichtliche Übersteigerung die vielen Menschen, die sich betroffen fühlen, nicht misstrauisch macht.

Entgegen dem, was die weltweite Kampagne gegen den ACTA-Entwurf behauptet, sind darin keineswegs bestimmte Maßnahmen vorgeschrieben, sondern es handelt sich eben nur um eine Aufforderung an die Vertragsstaaten, Durchsetzungsverfahren bereitzustellen. Und das Recht auf ein angemessenes Verfahren wird nicht beeinträchtigt, sondern es wird ausdrücklich gesagt, dass die entsprechenden Maßnahmen „fair“ und „gerecht“ sein und in „angemessenem“ Verhältnis zu der Schwere der Rechtsverletzung und den Interessen Dritter stehen müssen.[165] Viele der empfohlenen Instrumente sind schon Teil des deutschen Rechts. Geht es manchen Organisatoren der Kritik vielleicht doch in erster Linie um den Erhalt der wirtschaftlichen Vorteile, die sie aus der Verletzung von Urheber-, Marken- und verwandten Schutzrechten ziehen? Wenn eine Bürgerrechtsorganisation sich auf eine so maßlose Propaganda einlässt, macht sie sich unglaubwürdig; bei aller Kritik an der Ökonomisierung aller Lebensverhältnisse könnte sie wissen, dass die Menschenrechte nicht gerade durch ein solches rechtstechnisches Abkommen gefährdet sind.

Richtig ist freilich, was amnesty international anmerkt, dass nämlich die strengere Durchsetzung von Urheberrechten die Internetdiensteanbieter zu „repressiven Maßnahmen“ wie dem Sperren oder Löschen von Webseiten oder gar zum Ausschluss der Kunden von Dienstleistungen anreizen würde. Aber wäre es nicht genau richtig, wenn die Internetunternehmen – im Rahmen ihrer Erkenntnismöglichkeiten! – selbst darauf achten müssten, dass sie nicht zur Verletzung fremder Rechte beitragen? Es mag nicht immer leicht sein, insofern sichere Erkenntnisse zu erlangen, und selbstverständlich könnte über strittige Fälle vor den Gerichten gestritten werden. Wenn denn aber feststeht, dass angebotene Inhalte nicht verbreitet werden dürfen, können sich Anbieter wie Nutzer nicht auf Informations- oder Meinungsfreiheit berufen.[166] Beim Handel mit gestohlenen Büchern oder CDs würden wir von Hehlerei sprechen, und niemand würde sagen, die Händler müssten um der Meinungsfreiheit willen ermächtigt werden, die Augen fest zu schließen

164 Erklärung von amnesty international vom 13.2.2012, www.amnesty.de/2012/2/14/eu-darf-acta-nicht-unterzeichnen.

165 Art. 6 des Entwurfs.

166 S. a. Prantl 2012 mit der Klarstellung, dass das Urheberrecht ja nicht Informationen als solche, sondern „Werke“, also gestaltete Texte usw. schützt.

und alles als ehrliche Ware anzusehen. – Eine ganz andere Problematik wirft der Hinweis von amnesty auf die Versorgung mit Medikamenten auf: Würden Generika generell als Erzeugnisse von „Produktpiraterie" verstanden, so wäre das mit unserer Gesundheitspolitik unvereinbar. Das hat aber mit dem Streit um ACTA kaum etwas zu tun.

Eine Gruppe von Professoren aus verschiedenen Staaten – überwiegend aus Deutschland – hat in einer wohlabgewogenen Erklärung bemängelt, dass bestimmte Vorschriften in ACTA nicht mit dem geltenden europäischen Gemeinschaftsrecht vereinbar seien und/oder hinter den Standards des internationalen Rechts zurückblieben.[167] So sicherten einige ACTA-Regelungen keine ausreichende Abwägung zwischen den Interessen der Beteiligten oder es seien keine Maßnahmen vorgesehen, um die Durchsetzung der Vorbehalte und die Einhaltung der Grenzen der Befugnisse zu gewährleisten. Nötig seien z.B. spezifischere Vorschriften darüber, *wie* die Rechte auf Meinungsfreiheit, faires Verfahren und Privatheit effektiv gesichert werden sollen. Das sind rechtstechnische Details, die eher geringes Gewicht haben – zumal sich die Unterzeichner grundsätzlich zum Schutz der Rechte des geistigen Eigentums bekennen. Es ist ja durchaus wünschenswert, die Rechtslage aller Beteiligten möglichst eindeutig zu bestimmen, aber wo das Recht nur auf Prinzipien verweist, kann daraus nicht die Lösung aller denkbaren praktischen Fälle abgeleitet werden. Es unterhöhlt letztlich sogar die Geltungskraft von Rechtsvorschriften, wenn ihre Durchsetzung jeweils speziell vorgeschrieben wird – dass sie befolgt werden, ist selbstverständlich, und Selbstverständliches sollte nicht noch einmal normiert werden. Die zahllosen Absicherungswünsche signalisieren wohl nur, dass man der anderen Seite grundsätzlich misstraut. Solange das so ist, werden immer aufs Neue Nachbesserungen verlangt werden.

Die Piratenpartei bemerkt „mit Sorge", dass auch nach dem Scheitern von ACTA an internationalen Vereinbarungen über die Durchsetzung des Urheberrechts gearbeitet wird.[168] Im Kern ist der Interessenkonflikt zwischen Urhebern und Nutzern ungelöst. Dass er nicht einfach nach dem Prinzip entschieden werden kann, die „Netzfreiheit" genieße Vorrang, ist klar. Ebenso wenig wie die Auseinandersetzungen um Schmähungen und Mobbing im Netz allein zugunsten der Äußerungsfreiheit beendet werden können, ist das bei dem Konflikt um die Internet-Piraterie möglich. Das Urheberrecht hat immateriellen und zugleich materiellen Gehalt, es verschafft Künstlern, Autoren und Komponisten Anerkennung und Entgeltansprüche (während das Persönlichkeitsrecht zunächst immaterielle Ansprüche

167 Opinion of European Academics on Anti-Counterfeiting Trade Agreement, zugänglich auf der Internetseite des Instituts für Rechtsinformatik der Leibniz Universität Hannover, vgl. http://www.iri.uni-hannover.de/acta-1668.html.

168 Pressemitteilung v. 15.10.2012 zu Verhandlungen über ein Comprehensive Economic and Trade Agreement (CETA), s. www.piratenpartei.de . S.a. die Hinweise von Küchemann 2012 auf weitere europäische und amerikanische Rechtsetzungsinitiativen.

z.B. auf Unterlassung vermittelt und nur bei schweren Eingriffen auch Entschädigungen in Geld!). Das Recht derer, die geistige oder künstlerische Werke geschaffen haben, ist nicht weniger schutzwürdig als etwa die Gehaltsansprüche von Arbeitnehmern. Wie sollen sonst Künstler und Schriftsteller (und ihre Vermittler in Gestalt von Verlegern und Musikproduzenten) von ihrer Arbeit leben? Allein von dem Respekt anderer vor der eigenen Persönlichkeit kann niemand leben. Es ist also nicht einzusehen, dass die Leistungen der Journalisten, Schriftsteller und Künstler, die im Netz ausgestellt werden, nicht bezahlt werden sollen. Tatsächlich werden sie zum Teil ja über Werbeeinnahmen finanziert, so wie manche regionalen Wochenblätter, die unerbeten in die Briefkästen gesteckt werden, durch Anzeigen finanziert sind. Qualitätsjournalismus hat einen höheren Preis, und feste Abonnements sind eine solidere Basis als die schwankenden Reklameeinnahmen.

Alternative Regelungsmodelle

Da der Einzelne seine Vergütungsansprüche nicht allein durchsetzen kann, pflegt er die Ausübung seines Rechts einer Organisation, einem Verlag, Vertrieb oder einer Verwertungsgesellschaft (wie GEMA, VG Wort oder VG Kunst und Bild) zu übertragen, die dann einen Anteil an dem Entgelt erhält. Das erregt bei den Verfechtern der Unentgeltlichkeit Anstoß; sie halten diese Vermittler für Schmarotzer, die ohne eigene Leistung die Autoren und die Nutzer berauben. In manchen Fällen mag das zutreffen, in vielen anderen aber nicht; denn Verlage und Vertriebsfirmen müssen sehr wohl Geld aufwenden, um die künstlerischen und literarischen Leistungen zu vermarkten. Die rechtspolitische Aufgabe besteht darin, das Verhältnis zwischen Autoren und Vermittlern so zu regeln, dass beide Seiten zu angemessenen Erlösen kommen.

Diese Aufgabe ist nicht neu – es gibt ja ein ausgefeiltes Urheber- und Verlagsrecht und immer wieder Verbesserungen daran, und alle Seiten sind sich darin einig, dass die neuen Möglichkeiten der technischen Verbreitung von Inhalten zu neuen rechtlichen Gestaltungsformen führen müssen. Die Vergütungspflicht der Nutzer braucht auch nicht unbedingt an die einzelne Nutzung durch bestimmte Personen bzw. mittels bestimmter Computer anzuknüpfen. Es gibt bereits die *Geräteabgabe*: das (in gewissem Maße erlaubte) Kopieren von Texten und Bildern wird durch eine pauschale Abgabe vergütet, die der Hersteller, Händler oder Importeur von Kopiergeräten und Speichermedien oder der Betreiber von Kopiergeräten zahlen muss.[169]

169 §§ 53, 54, 54 b und 54 c Urheberrechtsgesetz.

Das Herunterladen von Texten oder Musik aus dem Internet ist technisch nicht dasselbe wie das „Ablichten“[170] aus Büchern oder das Abspielen von CDs, und es ist schwieriger, einen passenden Ansatz für die Vergütung von Downloads zu finden. Aber mit einiger juristischer Kreativität“[171] müsste ein Interessenausgleich auch auf diesem Felde möglich sein. Inzwischen haben sich darum schon viele Experten bemüht. So hat die Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages die in Betracht kommenden Vergütungsmodelle sorgfältig untersucht – ob es Werbefinanzierung, Flatrates oder Abonnements seien und an welche Nutzungsform sie zweckmäßig anknüpfen sollten. Die Empfehlungen waren freilich auch in der Kommission teilweise umstritten.[172] Jedenfalls wäre eine allgemeine „Kulturabgabe“, die von jedem Internetnutzer zu entrichten wäre, zumindest solange ungerecht, wie das Internet noch so unterschiedlich genutzt wird wie derzeit.[173]

Verschiedene Forschungsgruppen und Arbeitskreise sind ebenfalls mit detaillierten Erörterungen befasst, und die Öffentlichkeit verfolgt diese Debatten. Wenn dies alles zu Ergebnissen führt, die – vielleicht als alternative Entscheidungsvorschläge – zur Abstimmung gestellt werden können, ist ein wichtiger Schritt getan. Langfristig wird sich das Urheberrecht sicher noch vielfach ändern, und auch das kann einen Fortschritt bedeuten.

Freiheit vom Staat und Schutz durch den Staat

Grundrechtskonflikte und Interessenabwägungen

Wie auf allen Gebieten des Zusammenlebens, gelten auch für das Verhalten im Netz die Grundrechte des Einzelnen und der privaten Vereinigungen, ohne dass dies besonders festgelegt werden müsste. Für die Sphäre des Geschäftlichen sind die Grundrechte der Vertragsfreiheit, der Berufs- und Gewerbefreiheit, der Koalitionsfreiheit und des Eigentums von besonderer Bedeutung. Die unternehmerische Freiheit darf aus Gründen des Gemeinwohls eingeschränkt werden. Das Bundesverfassungsgericht hat diese Grundaussage in vielen Details ausgeformt und die Interessen der Unternehmer und der Allgemeinheit dabei sorgfältig austariert. „Eigentum verpflichtet“; „sein Gebrauch soll zugleich dem Wohle der Allgemeinheit

170 Das Gesetz spricht altmodisch von „Ablichtungsgeräten“.
171 Vgl. a. die Hinweise bei Güntner 2012.
172 Dritter Zwischenbericht der Enquete-Kommission, Bundestags-Drs. 17/7899 v. 23.11.2011, insbes. S. 45 ff.
173 So auch der Arbeitskreis Urheberrecht der SPD-Bundestagsfraktion, Positionspapier v. 21.5.2012: „Zwölf Thesen für ein faires und zeitgemäßes Urheberrecht“. Dazu u.a. ein Interview mit einem Fachjournalisten: www.thomas-steiger.com .

dienen“ (Art. 14 Abs. 2 GG). Die geistigen Freiheiten dürfen nur zugunsten höherrangiger Rechtsgüter eingeschränkt werden; eine Zensur ist ganz verboten. Das habe ich schon ausgeführt.[174]

Die Grundrechte schützen die Aktiven und die Passiven, je nach Bereich, und sie verpflichten den Staat sogar zum Schutz von Rechtspositionen der Individuen (z.B. gegen rechtswidrige Angriffe). Das Bundesverfassungsgericht hat dazu im Laufe der Zeit eine Lehre von den Schutzpflichten des Staates erarbeitet. In vielen Beziehungen stoßen Rechte und Interessen des einen auf solche eines anderen; zunächst können sich beide Seiten auf Grundrechtsartikel berufen. Der eine braucht Daten als „Rohstoff“ für seine geschäftlichen Aktivitäten, der andere will die Daten geheim halten, um seine Privatsphäre zu schützen oder wirtschaftliche Vorteile zu behalten, die ihm sein Wissensvorsprung bietet. Mit einer einseitigen Stellungnahme ist ein solcher Konflikt nicht zu befrieden. Deshalb müssen der Gesetzgeber und in zweiter Linie Verwaltung und Gerichte immer wieder *Abwägungen* vornehmen.

Was wäre, wenn der Staat sich überhaupt nicht mit all dem befassen würde, was im Internet geschieht? Die Vision der vollkommenen Staatsfreiheit muss jeden, der diesen Gedanken weiterdenkt, schaudern lassen. In den USA versuchen die Tea Party und große Teile der Republikaner gerade, den Staat handlungsunfähig zu machen. Die sozialen Folgen für die Mehrheit der Menschen sind erschreckend; noch erschreckender aber ist das Unvermögen der Menschen zu erkennen, dass sie immer mehr der Raffgier und Menschenverachtung derer ausgeliefert werden, die den „Markt“ steuern. Die Investoren, Finanziers und Manager, die nur den Gesetzen der Profitmaximierung folgen, gewinnen immer größere Freiheit und zahlen immer weniger Steuern, während die Masse der Arbeiter und Angestellten immer abhängiger wird. In Europa herrscht zum Glück bisher eine andere Vorstellung vom Verhältnis der Menschen zum Staat, aber die Bereitschaft, gemeinsame Angelegenheiten auch gemeinsam, also durch die kollektive Organisation Staat regeln zu lassen, nimmt auch hier ab. Der hochgelobte Philosoph Peter Sloterdijk propagiert die Abschaffung der Steuern zugunsten freiwilliger Gaben aller Wohlhabenden an die Allgemeinheit,[175] und manche Vordenker der „Piraten“ erklären alle Staaten und alle Politiker zu Feinden des Volkes, Verschwörern gegen das Allgemeinwohl.

Freundlich ausgedrückt, sind viele Verteidiger der totalen Internet-Freiheit liebenswerte Idealisten, die an das Gute im Menschen glauben und die dunklen Seiten der menschlichen Seele nicht wahrnehmen mögen. Wer sich stets an die Regeln hält, die das Zusammenleben in der Gemeinschaft erträglich machen, wird auch bei der Internet-Nutzung niemandem Schaden zufügen. Dass aber die Menschen,

174 S. oben S. 33 ff.
175 Dazu Bull 2011 d.

die für den Staat handeln, stets böse Absichten – Unterdrückung, Korruption, Machtmissbrauch – hätten, passt nicht zu dieser gedanklichen Basis der Menschenfreundlichkeit. Gewiss, die Funktionsträger der Allgemeinheit verwalten Macht, und Macht kann korrumpieren – aber dagegen gibt es Sicherungen, die in aller Regel wirksam sind, nicht zuletzt die Kontrolle durch Medien und Öffentlichkeit. Und die schroffe Gegenüberstellung von „gutem" Volk und „bösen" Politikern ist schon deshalb unerträglich naiv, weil sie übersieht, dass „gut" und „böse" wie Machtbesitz und Machtmissbrauch auf beiden Seiten vorkommen, in der privaten Gesellschaft und bei staatlichen Funktionsträgern.

Eine Politik, die die Freiheit der Einzelnen sichern will, ist auf den Staat angewiesen. Zwar können zivilgesellschaftliche Aktivitäten den Staat entlasten; viele Probleme würden gar nicht entstehen, wenn die Bürgerinnen und Bürger die Steine des Anstoßes selbst aus dem Wege räumten. Das geschieht aber nicht ausreichend und oft eben nicht in der richtigen Weise, und so muss der Staat als höchste Instanz der Gemeinschaft immer wieder korrigierend eingreifen.

Auch das Internet existiert nicht in einer absolut staatsfreien Welt. Der Wettbewerb stellt sich in der „realen" Welt nicht von selbst her, sondern muss vielfach erst geschaffen und immer wieder gefördert werden. Nicht anders ist es im Netz. Schon jetzt bilden die großen Vier Apple, Google, Amazon und Facebook ein Oligopol[176], und es ist nicht garantiert, dass die Netzwirtschaft so aufgeteilt bleibt wie sie gegenwärtig ist. Die Regulierung funktioniert international noch nicht effektiv genug, aber ohne staatliche Regulierung entsteht auf die Dauer Wildwuchs, was mit Sicherheit nicht den Individuen nützt. Auch Datenschutz, wie ihn die Netznutzer ja nachdrücklich wünschen, entsteht nicht staatsfrei. Selbst da, wo Unternehmen sich ohne behördliche Aufforderung zu Datenschutz und Datensicherung verpflichten, geschieht dies vor dem Hintergrund der Rechtsnormen, die ein entsprechendes Verhalten verlangen – Selbstverpflichtung „im Schatten des Rechts".

Theoretisch wäre es sogar denkbar, das Netz einer staatlichen oder internationalen bzw. supranationalen (EU-) Kontrolle zu unterstellen, die Betreiber also als öffentliche, nicht gewinnorientierte Unternehmen zu errichten. (Ob das zu besseren Ergebnissen führen würde als die gegenwärtige privatwirtschaftliche Ordnung, mag dahinstehen.) Eine Rechtspflicht, die grundlegenden Dienstleistungen der Telekommunikation allen Einwohnern zur Verfügung zu stellen, kann einem marktbeherrschenden Unternehmen nach deutschem Recht schon auferlegt werden, seit das Fernmeldewesen im Jahre 1994 privatisiert wurde. Zu dieser „Universaldienstleistung" ist gegenwärtig die Deutsche Telekom AG verpflichtet. An weitergehende Einflussnahme des Staates denkt zur Zeit niemand; die politischen Widerstände dagegen wären enorm.

176 „Die fanatischen Vier", Der Spiegel 49/2011, S. 70-81.

Über die Sicherung der Individualrechte hinaus müssen wir uns fragen: Wie kann das Allgemeininteresse gegen Fehlentwicklungen geschützt werden? Die Literatur zum Internet hat uns die Augen dafür geöffnet, dass auch Werte der Allgemeinheit gefährdet sind, wenn wir uns der Internet-Faszination unkritisch hingeben. Der „Cyber-Utopismus“ hat sich auch nach Ansicht prominenter Netz-Aktivisten als Enttäuschung erwiesen; sie sprechen vom „Netzwahn“[177] oder vom „kybernetischen Totalitarismus“[178] und setzen ihm einen „digitalen Humanismus“ entgegen.[179] Den gilt es auszugestalten, und dazu gehört die „Verbesserung“ der Demokratie, die Entwicklung einer aufgeklärten Medienkompetenz, der Schutz gegen Meinungsmonopole und Konformismus, der Schutz von Kindern vor Verführung und Missbrauch.[180] Die Verantwortung dafür, dass diese Ziele wirksam verfolgt werden, liegt beim Staat, nicht bei den Unternehmen. Die Wirtschaft ist aber als Teil der Gesellschaft sozialethisch in der Pflicht, den Boden dafür mit vorzubereiten und zu den notwendigen Maßnahmen das Ihre beizutragen.

Exkurs: „Lernen im Netz“ statt „Schule vor Ort“?

Wenn es nach den Ideen mancher Technikfreunde geht, werden auch Schulen und Hochschulen demnächst abgeschafft, weil das Lernen angeblich im virtuellen Raum besser organisiert werden kann als in den alten Gebäuden vor Ort. David Gelernter, der als Computerwissenschaftler in Yale lehrt und als jemand vorgestellt wird, der „die Grundlagen des World Wide Web“ geschaffen habe,[181] meint offenbar ernsthaft: „Die Flut, die den größten Teil der heutigen Schulen und Universitäten hinwegschwemmen und uns stattdessen ein netzbasiertes Bildungssystem ohne Schulen bringen wird, hat bereits begonnen“. Ein solches Bildungssystem hätte nach seiner Meinung „deutliche Vorzüge und hohe Kosten“. „Eltern, Schüler und Studenten werden aus einem weltweiten Bildungssystem auswählen können“; jeder kann in einem individuell angepassten Tempo lernen. Gelernter erkennt zwar an, dass „man am besten lernt, wenn Lehrer und Schüler einander direkt gegenüberstehen“, aber diese Art des Lernens werde man „weitgehend opfern“; denn die Großtechnologie werde sich gegen die Traditionen des Bildungswesens durchsetzen.

Hoffentlich nicht! Denn dieser Artikel ist ein Musterbeispiel dafür, auf welche Abwege jemand gerät, der eine politische und soziale Aufgabe allein von den technischen Möglichkeiten her lösen will, die auf dem Markt sind oder für die sich ein

177 Morozov 2011.
178 Lanier 2012, S. 30 ff.
179 Lanier 2012, S. 197 ff. S.a. die Rezension von H. Spiegel, FAZ v. 2.10.2010.
180 Zum Jugendschutz vgl. u.v.a. Ladeur 2000 S. 41 ff. („Toleranz reicht nicht [immer] aus“).
181 So die FAZ in der Autorennotiz zu Gelernter 2012.

Markt aufbauen lässt. Nicht einmal die höheren Kosten, die er selbst voraussagt, halten den Autor davon ab, seine Vorstellung von Online-Bildung zu verfolgen. „So denkt ein Technologe", kommentiert mit Recht die FAZ-Redaktion und macht darauf aufmerksam, dass sich das Bildungswesen „gegenüber technologischen Revolutionen bislang als äußerst träge erwiesen" hat.[182] Bisher herrscht noch weitgehend Konsens darüber, dass die Schule ein *sozialer Ort* ist, an dem nicht nur Stoff gelernt, sondern auch soziales Verhalten geübt werden soll. Wie heißt es doch so schön: „Die Schule der Demokratie ist die Schule". Die Online-Schule kann das nicht sein. Wer vorrangig auf das individuelle Lernen im und am Netz setzt,[183] verkennt Grundeinsichten jeder Didaktik. Gewiss müssen wir das Schul- und Hochschulsystem immer wieder radikal kritisch überprüfen und dabei auch die Chancen des Lernens im Netz einkalkulieren. Aber es ist unwissenschaftlich und anmaßend, das Bildungswesen und die Lehrer (in aller Welt!) pauschal zu disqualifizieren und allein von der Technik her ein ideales neues System zu konzipieren.

Das Netz und die Netze: Neutralität, Kapazität und Sicherheit der Datentechnik

Was bedeutet Netzneutralität?

Zur „Freiheit des Internet" gehört nach Ansicht von „Piraten" und anderen Netz-Begeisterten das Prinzip der Netzneutralität.[184] Darunter versteht man, dass alle über das Netz zu transportierenden Datenpakete gleich behandelt werden, also weder eine Priorisierung nach Inhalten noch nach Art der Daten erlaubt ist. Wer zuerst kommt, wird zuerst bedient; in der Sprache der Informatiker: „Best-Effort-Prinzip" und „First-In/First-Out-Prinzip". „Bei Übertragungsengpässen entscheidet allein die zeitliche Reihenfolge der anfallenden Transportvorgänge darüber, welcher Vorgang zuerst abgewickelt wird".[185] Das ist zweifellos ein angemessener Grundsatz, solange die Engpässe allenfalls vorübergehender Natur sind und die Kapazitäten ständig erweitert werden, und überdies ein Prinzip, das die Gleichheit der Individuen betont und damit auch demokratiefreundlich zu sein scheint. Es bestärkt anscheinend auch den lakonischen Satz des Grundgesetzes: „Eine Zensur findet nicht statt" (Art. 5 Abs. 1 Satz 3 GG).

182 Ebd. („kau").
183 So auch Beckedahl/Lüke 2012, 79 ff. Besonders irreal ist deren Vorstellung, die Studierenden würden künftig mit ihren Laptops jederzeit „gegenprüfen", ob der Dozent richtig zitiert und „auf dem aktuellen Stand der Forschung" ist. Das Abrufen von Informationen aus dem Netz ist noch lange kein Lernen und schon gar nicht Anleitung zu kritischem Denken.
184 Vgl. dazu die Beiträge in Kloepfer 2011.
185 Eberle 2011, S. 979 ff. (980) (m.w.N.).

Aber das so verstandene Prinzip der Netzneutralität ist nicht selbstverständlich und wahrscheinlich nicht auf Dauer durchhaltbar. Je mehr Datentransporte auf das Internet verlagert werden, desto mehr Engpässe wird es geben. Längst werden ja nicht mehr überwiegend E-Mails verschickt und individuelle Bestellungen abgewickelt. Gewaltige Kapazitäten sind erforderlich, um die massenhafte Auftragsdatenverarbeitung, die Internet-Telefonie, Software-Downloads, Online-Spiele und Videodarbietungen zu ermöglichen. Das Livestreaming, die zeitgleiche Verbreitung von Fernsehprogrammen, ist überaus aufwendig, ebenso das zeitunabhängige On-Demand-Streaming etwa aus Mediatheken. Global vernetzte Produktionsprozesse sollen ebenso zuverlässig abgewickelt werden wie komplizierte Operationen, die internet-gestützt von Ärzten in weit entfernten Kliniken kooperativ durchgeführt werden.

Niemand hätte wohl etwas dagegen einzuwenden, wenn zwischen dem Angebot von Online-Spielen und der Übertragung von Operationsdaten unterschieden würde. Notrufe, Gesundheitsdienstleistungen und Katastrophenhilfe sind allemal dringender als das Angebot von Unterhaltungsprogrammen. Der wirtschaftlichen Logik entspräche es ohnehin, wenn unterschiedlich wichtige Datentransporte auch unterschiedlich bezahlt werden müssten – wir sind ja auch bereit, für eingeschriebene Sendungen ein Extraentgelt zu zahlen. Einer bevorzugten Behandlung beim Internettransport entspricht es, dass wir Briefe und Pakete per „Eilboten“ zustellen lassen – selbstverständlich gegen Sondergebühr. Als verbotene Priorisierung gilt nach dem Netzneutralitätsprinzip schon, dass eine Sendung um Bruchteile von Sekunden verzögert transportiert wird. Für die Qualität der Bild- und Tonübertragung kann das schon eine Rolle spielen. Aber Überlegungen, unterschiedliche Qualitätsstufen (-klassen) einzuführen, sind in der Welt. Einige Unternehmen wollen sich offenbar die bessere Qualität der Übertragung zusätzlich bezahlen lassen. Andere halten dagegen, insbesondere die Fernseh- und Videoanbieter, die an der höchstqualifizierten Transportmethode interessiert sind.

Sollten die Internetdienste eines Tages tatsächlich nach Maßgabe der „Quality of Services“ differenziert werden, wird auch die Frage wieder aufgeworfen, ob nicht damit der Zensur das Tor geöffnet wird. Das verfassungsrechtliche Zensurverbot richtet sich zwar nur an den Staat und nicht an private Internetunternehmen, aber die Freiheit der Kommunikation muss auch gegen die Macht der Internetbetreiber verteidigt werden. In der Aufstellung eines differenzierten Preiskatalogs für unterschiedliche Arten von Datentransport läge freilich noch kein Verstoß gegen das Zensurverbot; es muss nur sichergestellt werden, dass eine eventuelle Staffelung nicht nach den Inhalten der Datenpakete, sondern nach der Art und dem Zweck der Datentransporte vorgenommen wird – möglichst nach technischen Merkmalen, nach denen unterschiedliche Inhalte gleich behandelt werden. Möglicherweise wird eine zusätzliche Kennzeichnung der Pakete nötig sein: individuelle private

Sendungen (auch an eine Mehrzahl von Empfängern) könnten anders markiert werden als Massendatenpakete zur Weiterverarbeitung, Fernseh- und Videosignale würden eine eigene Datenklasse bilden, und falls auch innerhalb dieser Klasse eine vorrangige Behandlung nötig werden sollte – z.B. für Notfälle wie die fernsehtechnische Assistenz beim Katastrophenschutz und anderen Hilfseinsätzen –, müssten Ausnahmen dafür durch entsprechende technische Qualifizierung ermöglicht werden. Natürlich ist das keine leichte Aufgabe, aber eine lösbare.

Die Internet-Nutzer hätten verständlicherweise die Sorge, dass die Betreiber ihre Leistungen zu teuer verkaufen. Diese stehen aber unter der Aufsicht der Kartellbehörden und der Gerichte, die auch auf diesem Feld eventuellen Auswüchsen mit den Instrumenten des Verbraucherschutzes begegnen können. Die Bundesnetzagentur als zuständige Sonderkartellbehörde für das Netz hat gesetzliche Befugnisse, die sie in diesem Fall aktivieren könnte.[186]

Die Störanfälligkeit des Netzes

Unsere vernetzte Welt wird „immer störanfälliger".[187] Wenn eines Tages das Internet zusammenbricht, wird es in Teilen der Welt zappenduster, weil die Elektrizitätswerke ausfallen, und überall bleiben Bahnen, Fließbänder und Aufzüge stehen, kurz: alle Anlagen werden funktionsunfähig, die mit externen Computern verbunden sind. Wirtschaft und Verwaltung sind so sehr vom Netz abhängig, dass ein großer Teil der normalen Geschäftstätigkeit nicht mehr ohne dieses Instrument bewerkstelligt werden kann. Sabotageakte und Hackerangriffe machen schon jetzt vielen Unternehmen und Behörden schwer zu schaffen, und als Außenstehender wundert man sich, dass dieses Risiko von den Betreibern gering eingeschätzt wird. Als mögliche Ursachen sind aber auch Stromstörungen, Schlampereien, Überlastung und Fehlschaltungen zu bedenken,[188] und die Folgen könnten für große Teile von Wirtschaft und Verwaltung verheerend sein.

Es gibt keinen zuverlässigen Schutz gegen eine solche Katastrophe. Es ist leicht, sich darüber zu mokieren, dass die zur Kontrolle der Informations- und Kommunikationstechnik eingesetzten Behörden personell schwach sind.[189] Die Verantwortung für das Funktionieren des Internets liegt bei denen, die es aufgebaut haben, betreiben und nutzen, und die Behörden dürfen erst eingreifen, wenn gegen Rechtsnormen verstoßen wird. Gleichzeitig machen sich die hochgelobten Hacker – üb-

186 Vgl. Schwarz-Schilling 2011, S. 133 ff. Zu den europarechtlichen Bindungen auf diesem Gebiet: Mayer 2011, S. 81 ff.
187 Fischermann/ Hamann 2012.
188 Über frühere Zwischenfälle und Pannen im Netz berichten anschaulich z.B. Fischermann/ Hamann 2012, z.B. S. 13-15.
189 So etwa Fischermann/Hamann 2012, S. 202 ff.

rigens auch sie nur eine kleine Schar von Menschen – über die Behörden lustig und werden dafür von manchen Medien noch belobigt. Dem Staat mangelnde Vorsorge gegen Störungen und Pannen vorzuwerfen, ist also allzu billig, zumal wenn gleichzeitig behauptet wird, die Behörden wüssten zu viel über die Menschen. Der Staat weiß eben nicht alles, und wir wollen es so.

Ein Patentrezept hat offenbar bisher niemand. Man hofft, dass die Katastrophe nicht eintreten oder dass sie nur andere treffen werde; bestenfalls werden Notaggregate vorgehalten. Sicherheit gegen Angriffe oder gegen Stromausfälle und Kabelzerstörung scheint es nicht zu geben. Wer insofern auf den Staat oder die Staatengemeinschaft hofft, macht sich Illusionen. Die privaten Betreiberunternehmen haben ein starkes eigenes Interesse daran, dass das Netz leistungsfähig bleibt, und sie tun viel für die Sicherheit ihrer Anlagen. Der Staat könnte das wohl kaum besser, obwohl er kein Profitinteresse hätte und daher (vielleicht) niedrigere Kosten verursachen würde.

Das Netz und die Netze

Eine Chance, etwas mehr Funktionssicherheit der Datenverarbeitung und der elektronischen Kommunikation zu gewinnen, besteht darin, das eine große Netz in verschiedene, voneinander getrennte Netze aufzuteilen. In manchen Bereichen könnte ganz auf die Vernetzung verzichtet werden. Isolierte Systeme sind besser gegen Eingriffe von außen und Netzstörungen geschützt. So nahe diese Lösung auch liegt, sie ist bisher nur in bescheidenen Ansätzen und offenbar halbherzig verwirklicht.

Die WikiLeaks-Enthüllungen haben offengelegt, dass sogar die amerikanische Armee und das US-Außenministerium viel zu viele Zugriffsmöglichkeiten auf ihre internen Nachrichtennetze zugelassen oder ermöglicht haben. Dass andererseits auch solche Dateien, die nur für einen kleinen Kreis von Personen von Interesse sind, im weltweiten Netz gespeichert werden, war schon immer fragwürdig. Warum müssen Dozenten und Studenten einer deutschen Universität miteinander über Server in Amerika kommunizieren? Warum werden die Programmdaten eines Stadttheaters und der Fahrplan eines örtlichen Verkehrsunternehmens durch Überseekabel oder Satelliten um die Welt gelenkt, ehe sie bei den Interessenten „nebenan“ eintreffen? Ist es nötig, dass meine Verbrauchsdaten, die nur für den regionalen Stromversorger bestimmt sind, über das Internet transportiert werden? Führt die ökonomische Logik zwingend zur Verarbeitung von Datenmassen aus aller Welt bei beliebig entfernten Rechenzentren?

Denken wir daran, dass auch höchst gefährliche und gefährdete industrielle Anlagen, Atomkraftwerke und das Stromnetz ebenso wie Verkehrsleitanlagen und die

Flugsicherung durch Computer gesteuert werden, die an das Internet angeschlossen sind, so kann uns angst und bange werden. „Solche kritischen Infrastrukturen, die wir für unseren Alltag dringend brauchen, bei denen es um Leben und Tod geht – sie müssen unwiderruflich vom Netz".[190]

Aber auch sonst liegt es nahe, das einheitliche World Wide Web von vielen Anwendungen zu entlasten, die nur lokale oder regionale Bedeutung haben, und diese in eigene, speziell zweckbestimmte Netze zu überführen.[191] Damit ist nicht gemeint, dass das Netz vollständig zerlegt, vor allem nicht dass es in die Hände der nationalen Regierungen gelegt werden soll, die dann ihr Territorium „perfekt" von dem weltweiten Netz abkoppeln könnten. Wir dürfen die große Errungenschaft eines globalen Informations- und Kommunikationsmediums ohne nationale Grenzen nicht aufgeben. Eine – immerhin denkbare – Vorschrift der Europäischen Union, dass die Daten über Europäer nur in Europa gespeichert werden dürfen,[192] wäre ebenfalls ein Rückschritt. Aber eine nach Zwecken und Teilnehmerkreisen differenzierte Datenverarbeitung könnte durchaus freiheitsfreundlich gestaltet werden – ginge es doch auch um eine Form von „informationeller Gewaltenteilung". Dieses seit den Anfängen des Datenschutzes bekannte Prinzip wird oft vernachlässigt.

Der freie Zugang zu allen großen und kleinen Wissens-Portalen und Diskussionsforen könnte dabei ohne weiteres gewährleistet bleiben, solange eben nicht nationale Regierungen die Herrschaft darüber gewinnen. Die Sicherheit und Zuverlässigkeit der Systeme aber würde deutlich erhöht, und damit würde vielen Ängsten der Boden entzogen, die in unserer Gesellschaft herrschen.

190 Fischermann/Hamann 2012, S. 246.
191 So auch Fischermann/Hamann 2012, S. 243 ff.
192 Als Denkmodell bei Fischermann/Hamann 2012, S. 243.

Dritter Teil: Neue Formen der Demokratie

Der weltweite Protest und die Ziele der Internet-Demokraten

Überall in der Welt entstehen Protestbewegungen gegen soziale Ungerechtigkeit, gegen autoritäre Regierungen, gegen Raffgier und Verschwendungssucht von Unternehmen und Raubbau an der Natur. *Stephane Hessels* Appelle „Empört euch!" und „Engagiert euch!" sind europaweit verbreitet. Für Hessel ist die soziale Gerechtigkeit das höchste Ziel; er hat es schon als Resistance-Kämpfer gegen die deutsche Besetzung Frankreichs verfochten. Sie muss immer wieder neu erkämpft werden. Die *Occupy*-Bewegung hat den massenhaften Widerspruch gegen die Macht der Banken zum Ausdruck gebracht, die ganze Volkswirtschaften in den Ruin zu treiben scheinen. Verglichen damit, sind die Klagen über das Internet und die Computerisierung der Welt nur schwach vernehmbar. Erstmals fanden Demonstrationen gegen den Ausbau der Sicherheitsbehörden statt, bei denen auch die Informationstechnik eine Rolle spielte: Unter dem Motto *„Freiheit statt Angst"* versammelten sich viele Tausend Menschen, um gegen die Vorratsdatenspeicherung und ähnliche Instrumente der Sicherheitspolitik zu protestieren.

Motive und Ziele der Protestbewegungen sind aber noch verschwommen und dringend diskussionsbedürftig, und dementsprechend herrscht auch in der Internet- und Datenschutzdiskussion weitgehend Unklarheit über Ziele und Konsequenzen, und bei genauerer Betrachtung sind einige Ziele offensichtlich unerreichbar.

Transparenz der Politik, informierte Bürger

Transparenz, Partizipation und bessere Politik – das sind die zentralen Ziele der „Internet-Demokraten". Man könnte seitenlang euphorische Äußerungen verschiedenster Autoren zitieren, die einen grundlegenden Wandel der politischen Strukturen und Prozesse prophezeien. Auch seriöse Medien wie „Zeit" und „Spiegel" verbreiten die These, das Netz könne die Gesellschaft „demokratisieren" und die Welt „transparenter" machen.[193] Glaubt man ihnen, dürfen wir hoffen, dass das allen Menschen offenstehende Internet in absehbarer Zeit eine bessere Welt schafft.

193 Eine kurze Darstellung der Wellen „überhöhter Transformationshypothesen" und dazwischen liegender Phasen der Desillusionierung („Hype-Zyklen") findet sich bei Schrape 2010, S. 13 ff.; dort auch die Zitate im Text.

Sind diese Hoffnungen realistisch? Oder zerfallen sie bei näherem Hinsehen zu Hirngespinsten?

Die Menschen, die diese Hoffnungen hegen und die uns deshalb das Internet als Heilmittel der Demokratie empfehlen, schließen aus den bestehenden technischen Möglichkeiten auf die Realisierbarkeit politischer und sozialer Reformen. Sie sind optimistisch genug anzunehmen, dass

- die allermeisten Mitmenschen dieselben Wünsche und Prioritäten haben wie sie selbst, also „alles" wissen und möglichst viel mitbestimmen wollen, und dass sie
- dafür bereit sind, sich der neuen Techniken intensiv zu bedienen,

und sie sind überzeugt, uns damit tatsächlich dem Ziel näher zu bringen, dass

- der größere Teil der Menschen seine politische, soziale, ökonomische und kulturelle Umwelt klarer durchschaut als vorher,
- dass die Bürgerinnen und Bürger (ständig und auch ohne besonderen Anlass wie die verfassungsmäßigen Wahlen und Abstimmungen) ihre eigenen Angelegenheiten intensiver, sorgfältiger und mit mehr Verbindlichkeit wahrnehmen als ohne die neuen Instrumente und
- dass dabei am Ende eine höhere Qualität von Entscheidungen entsteht, es also schließlich allen besser geht und die großen Risiken der Entwicklung gebannt werden können.

Nur wenn die Voraussetzungen – gleiche Präferenzen und gleiches Engagement – zutreffen, kann das Ziel erreicht werden, und damit sind noch keineswegs alle Bedingungen einer anspruchsvollen Form von Demokratie angegeben. Zu denken ist an das Vorhandensein allgemeiner und politischer Bildung bei möglichst vielen Menschen, an die Einstellungen und Verhaltensmuster der Menschen. Man kann mit guten Gründen bezweifeln, ob diese (durch den Staat kaum zu schaffenden, jedenfalls nicht allein durch Rechtsnormen zu erzeugenden) Voraussetzungen typischerweise gegeben sind. Aber auch wenn ich mich auf die beiden bezeichneten Punkte konzentriere: Ich bin mir nicht sicher, ob sie wirklich gegeben sind.

Auf den ersten Blick scheint es selbstverständlich und keines Beweises bedürftig, dass wir möglichst viel wissen und möglichst viel mitbestimmen wollen. Als kritische Bürger interessieren wir uns für alle möglichen Unterlagen, die in der staatlichen Verwaltung vorhanden sind und der Vorbereitung von Verwaltungshandeln, Planungen und Entscheidungen dienen: Gutachten und Entwürfe, Protokolle, Statistiken und ganze Akten zu einzelnen Verwaltungsvorgängen. So wollten Berliner Bürger den Privatisierungsvertrag des Senats mit den Wasserbetrieben lesen, um etwaige Versäumnisse oder Fehler der Verhandlungsführer zu erfahren oder einfach um ihr Misstrauen gegen Privatisierungen bestätigt zu erhalten. Das

dazu in Gang gesetzte Volksbegehren hatte Erfolg, Nach dem Volksentscheid vom 13.2.2011 hat das Berliner Abgeordnetenhaus am 4.3.2011 das Gesetz für die vollständige Offenlegung von Geheimverträgen zur Teilprivatisierung der Berliner Wasserbetriebe erlassen. Die Verträge wurden im Amtsblatt für Berlin veröffentlicht und sind über das Internet-Portal des Berliner Beauftragten für Datenschutz und Informationsfreiheit öffentlich zugänglich. In einer anderen Stadt mag sich das Interesse auf die Korrektheit eines Liefervertrages oder der Einstellung eines Mitarbeiters richten. Oft wird Korruption vermutet und soll durch Informationsfreiheit verhindert oder aufgeklärt werden.

Zehn deutsche Länder und der Bund haben Informationsfreiheitsgesetze geschaffen, die das Wissen der Verwaltung weitgehend für jeden nutzbar machen, der sich dafür interessiert.[194] Das waren demokratische Großtaten: Es war um der Beteiligung der Bürger willen zwingend geboten, die Tradition des Obrigkeitsstaates zu beenden. Der demokratische Staat darf sich nicht in einem „Arkanraum" verschanzen.[195] Das Recht, sich über das Wissen und die Absichten der Behörden zu informieren, wird tatsächlich von vielen Einwohnern wahrgenommen, freilich von unterschiedlichen Gruppen in unterschiedlicher Intensität und in Deutschland, verglichen mit anderen Staaten, „eher zurückhaltend".[196] Politisch interessierte Mitbürger bedienen sich dieses Rechts häufiger als diejenigen, die nur in einem sie betreffenden Fall Näheres wissen wollen. In manchen Kommunen wird regelmäßig nachgefragt, in anderen selten oder nie. Häufig nutzen Journalisten und Zeithistoriker die Möglichkeit, Genaues über das Innenleben der Behörden zu erfahren. Bürgerinitiativen und Interessenverbände bilden eine weitere Nutzergruppe.[197]

Der Anspruch auf Akteneinsicht wird auch durch die Landesbeauftragten für den Datenschutz unterstützt und kann notfalls vor den Verwaltungsgerichten durchgesetzt werden. Das Land Hamburg hat darüber hinaus ein „Transparenzgesetz" erlassen, das die Behörden dazu verpflichtet, von sich aus – also auch wenn niemand dies beantragt hat – alle politisch bedeutsamen Informationen zu veröffentlichen.[198] Danach werden u. a. „Verträge der Daseinsvorsorge", „Haushalts-, Stellen-, Bewirtschaftungs-, Organisations-, Geschäftsverteilungs- und Aktenplä-

194 Als erstes Land hat Brandenburg bereits 1998 ein „Akteneinsichts- und Informationszugangsgesetz" beschlossen, ihm folgten Berlin 1999, Schleswig-Holstein 2000, Nordrhein-Westfalen 2001, der Bund 2005 und die Länder Bremen, Hamburg, Mecklenburg-Vorpommern und Saarland 2006, Thüringen 2007, Sachsen-Anhalt sowie Rheinland-Pfalz 2008. Das Bundesgesetz ist kommentiert u.a. in: Schoch 2009; dort auch Abdruck der bis dahin zehn Landesgesetze. Nur die Länder Bayern, Baden-Württemberg, Hessen, Niedersachsen und Sachsen haben noch kein Gesetz über den Zugang zu den Informationen der Verwaltung zustande gebracht.

195 Grundlegend dazu Wegener 2006.

196 Schaar/Roth 2012, S. 5.

197 Einzelheiten dazu u.a.in den Berichten der Landes- und des Bundesbeauftragten für (Datenschutz und) die Informationsfreiheit und bei Lukaßen 2010.

198 Hamburgisches Transparenzgesetz v. 19.6.2012, HmbGVBl. S. 271.

ne“, Verwaltungsvorschriften, Statistiken, Tätigkeitsberichte, Gutachten und Studien, Geodaten, Subventions- und Zuwendungsvergaben sowie „die wesentlichen Unternehmensdaten städtischer Beteiligungen einschließlich einer Darstellung der jährlichen Vergütungen und Nebenleistungen für die Leitungsebene“ in ein allgemein zugängliches elektronisches „Informationsregister“ eingegeben.

Es ist aber unmöglich, alle beim Staat vorhandenen Informationen für alle Einwohner offen zu legen. Schon die betroffenen Privaten würden dagegen heftig opponieren. Dass daher Ausnahmen von der obligatorischen Offenlegung aller Verwaltungsvorgänge geboten sind, ist zwingend. Die Ausnahmebestimmungen der Informationsfreiheitsgesetze sind unterschiedlich ausgestaltet, aber im Kern ähneln sie sich alle. Schon der historische Vorläufer, der amerikanische Freedom of Information Act, nimmt in neun Klauseln eine ganze Reihe von Fällen aus legitimen Gegeninteressen von der Offenlegungspflicht aus. Auch das Hamburgische Transparenzgesetz enthält selbstverständlich Ausnahmeklauseln zum Schutz personenbezogener Daten und von Betriebs- und Geschäftsgeheimnissen sowie für einige besonders sensible Bereiche (z.B. Steuerfestsetzung und -erhebung, allgemein für Rechtspflegeorgane, Disziplinarbehörden und Vergabekammern). Was für Ermittlungsverfahren von Justiz und Polizei gilt, dass man den möglichen Betroffenen nicht vorab aufdecken kann, was man über sie weiß, gilt auch für andere Verwaltungsvorgänge: Auch die Verstöße gegen Umweltschutzrecht und Lebensmittelhygiene müssen im Frühstadium nicht-öffentlich verfolgt werden, und solche Beispiele ließen sich vervielfältigen. Die Behörden brauchen ihre Strategie zur Durchsetzung der Rechtsnormen nicht auf dem offenen Informationsmarkt bekannt zu geben, solange die Wirksamkeit von der Geheimhaltung abhängt.

Konfliktfrei geht die Erfüllung von Informationsbegehren keineswegs vor sich. Viele Behörden hüten ihre Geheimnisse, so lange es möglich ist, bisweilen unter grober Verletzung der Gesetzesnormen. Die Informationsfreiheitsbeauftragten berichten von mancherlei Widerstand gegen begründete Informationsanträge, und die Verwaltungsgerichte sind schon des Öfteren mit solchen Klagen befasst worden; meistens haben sie den Petenten gegen die Verwaltung Recht gegeben.[199]

Wird die begehrte Auskunft gegeben, so ist damit allein das politische Klima noch nicht bereinigt. Sofern jemand hoffen sollte, die Offenlegung bisher vertraulicher Unterlagen werde sogleich der politischen Vernunft zum Erfolg verhelfen, würde dieser schnell enttäuscht. Auch über „transparente“ Verhältnisse kann und wird regelmäßig gestritten. Am ehesten bewirkt die Offenlegung etwas, wenn kon-

199 So hat das BVerwG klargestellt, dass grundsätzlich auch ministerialinterne Vermerke für die Ministerin oder den Minister offenzulegen sind. Das Verlangen nach einer Ausnahme (über die im Gesetz enthaltenen hinaus) zeichne „das Bild einer Ministerialverwaltung mit einem eher geringen Selbstbewusstsein“ (BVerwG, U. v. 3.11.2011). Einen ähnlichen Fall einer parlamentarischen Auskunftspflicht hat das BVerfG ebenfalls zugunsten der Öffentlichkeit entschieden (BVerfGE 110, 199).

krete Vorwürfe gegen Amtsträger auftauchen. Sachfragen sind meist so komplex, dass sie infolge unterschiedlicher Interpretation der Sachverhalte nicht eindeutig entschieden sind, wenn „die ganze Wahrheit" zutage tritt.

Genaue Folgenbetrachtung führt also zu Zweifeln an den praktischen Folgen der Transparenz.[200] Dass möglichst viele Menschen möglichst „alles" über das Handeln der Politiker wissen sollen, ist im Grunde nur eine vereinfachte Formel für die gut demokratische Forderung, die Politiker besser zu kontrollieren; Informationsansprüche sind dazu hilfreich. Aber die Kontrolle der öffentlichen Angelegenheiten hängt eben nicht einfach davon ab, wie viel die Öffentlichkeit weiß. Manche kritischen Punkte sind bestens bekannt und werden doch nicht kritisiert; erst bei epidemischer Ausbreitung und entsprechenden Schadensfolgen werden sie aufgegriffen. Andere verursachen Stürme im Medienwald, obwohl sie längst aufgeklärt sind, und oft werden aus Spekulationen und Vermutungen schwerwiegende Vorwürfe abgeleitet, die leicht widerlegt werden können. Wir sind als Gesellschaft offensichtlich nicht mehr in der Lage, die Fülle der verfügbaren Informationen zu verarbeiten und ihre Bedeutung angemessen zu gewichten. So erscheint es wie Willkür, wenn aus der Menge des täglich Berichteten auf unerklärliche Weise mediale Skandale entstehen, und wir laufen Gefahr, dass das Wichtigste und Gefährlichste unbeachtet bleibt. Mag sein, dass die Aufdeckung geheimer Unterlagen dieses Risiko ein wenig verringert, aber der Wert von Publizität und Transparenz bleibt begrenzt.

Das Mittel Transparenz darf jedenfalls nicht zum Selbstzweck werden, es darf nicht „hundertprozentig" angewendet werden. Auch das Geheimnis hat seinen demokratischen Wert. Skeptiker gehen in ihrer Kritik noch weit über die praktischen Gegengründe hinaus. So ist die heutige „Transparenzgesellschaft" für den Sozialphilosophen Byung-Chul Han auch eine „gleichgeschaltete Gesellschaft" und eine „Kontrollgesellschaft".[201] Bezweifelt wird sogar, dass sie Vertrauen schafft.[202] Wenn das zutrifft, bricht ein zentrales Element aus dem Wertesystem vieler Internetnutzer heraus.

Enthüllungsplattformen und Open Government

Dass selbst sensationelle Entdeckungen nicht ohne weiteres die Welt verändern, hat die Geschichte der Enthüllungsplattform *WikiLeaks*[203] gezeigt. So hätte man glauben können, das ins Internet eingestellte furchtbare Video aus dem Irak-Krieg,

200 Grundlegend kritisch auch Han 2012. S. a. Wewer 2012.
201 Han 2012, S. 7 und 74 ff.
202 Krastev 2012.
203 Dazu: Rosenbach/Stark 2011 sowie Geiselberger 2011.

in dem gezeigt wird, wie eine Hubschrauberbesatzung unbeteiligte Zivilisten tötet und dabei zynische Sprüche von sich gibt, würde eine weltweite Empörung und harte Reaktionen der Verantwortlichen auslösen. Aber empört haben sich nur kleine Teile der globalen Öffentlichkeit und wohl nur außerhalb der USA. Die Debatte um Sinn und Unsinn des Irak-Krieges verlief fast unbeeinflusst von den schauderhaften Bildern; die Positionen standen vermutlich schon vorher fest, und wir wissen nichts darüber, wie viele Menschen etwa ihre ursprünglich positive Einschätzung des amerikanischen Unternehmens revidiert haben. Die Offenlegung geheimer Unterlagen aus dem Afghanistan-Krieg ist sogar auf Kritik gestoßen, weil dadurch Informanten oder Betroffene gefährdet worden seien. Die Veröffentlichung der vertraulichen diplomatischen Korrespondenz des State Department schließlich hat zwar Kritik an Stil und Methode der amerikanischen Außenpolitik provoziert, aber im Grunde hat man bald erkannt, dass jeder Staat von seinen Diplomaten ungeschminkte Urteile über die ihnen begegnenden Personen erwartet – Einschätzungen, die nicht für die Öffentlichkeit geeignet sind. Die unzensierte Transparenz erweist sich hier also gerade nicht als demokratisches Wunschbild, sondern als unnötiger Störfaktor in den internationalen Beziehungen.

Radikale Verfechter von „Open Government" meinen, dass die Regierungen in aller Welt im Kern nichts anderes im Schilde führen als Verschwörungen gegen das Volk. Sie unterstellen sämtlichen Politikern, dass sie nur ihre eigenen Interessen verfolgen und dem Volk schaden wollen. Schon zur „Philosophie" der ersten prominenten Hacker gehört das Motto, allen Autoritäten zu misstrauen.[204] Der WikiLeaks-Gründer Julian Assange „kämpft gegen den Staat als Sammelbecken einer vermeintlich korrupten Elite"; er sieht in den Medien, der Wirtschaft und der politischen Elite eine „Verschwörung gegen die Bürger".[205] Wer so redet, kann als demokratischer Politiker nicht ernst genommen werden. Wer nur Feindbilder pflegt, wer glaubt, nur durch Machtpolitik die Welt verbessern zu können, macht sich politikunfähig. Es ist die Attitüde dessen, der sich im Besitz der Wahrheit und der einzig richtigen Idee von Gerechtigkeit glaubt. Solche Menschen haben in der Geschichte zwar immer wieder Diktaturen errichtet (oder es versucht), aber keine Demokratien. Denn Demokratie ist die Staatsform des Pluralismus und der Relativität der Meinungen und Kräfte.

Geradezu grotesk wird die Selbstüberschätzung eines vermeintlich Fortschrittlichen, wenn er das Spannungsverhältnis von Transparenz und Privatsphäre mit Hilfe der Trennung zwischen Reich und Arm auflösen will. *Pavel Mayer*, einer der ins Berliner Abgeordnetenhaus gewählten „Piraten", schlägt dies ernsthaft vor: „In einer Gesellschaft, in der ich leben möchte, kann da, wo der materiell Starke und

204 Rosenbach/Stark 2011 S. 106 f. zitieren ein entsprechendes „Hacker-Manifest" von Steven Levy aus dem Jahre 1984.

205 Zitate bei Rosenbach/Stark 2011, S. 109.

Mächtige dem Schwachen gegenübertritt, der Schwache den Schutz des Geheimnisses beanspruchen. Der Starke ist demgegenüber in der Pflicht, sich allein durch objektives und transparentes Handeln zu rechtfertigen". Deshalb habe der Staat „als besonders starke Macht" „besondere Zurückhaltung zu üben, wenn er sich durch Geheimnisse schützen will, während der Einzelne selbstverständlich das Recht hat, sein Tun zu verheimlichen".[206]

Mayer vergleicht also den Einzelnen, der angeblich (immer?) schwach ist, mit dem angeblich (immer?) starken Staat, einem Abstraktum, das zwar juristisch eine Einheit darstellt, faktisch aber in eine Vielzahl von Akteuren und Systemen zerfällt, die untereinander um Macht und Einfluss ringen und die vor allem große Mühe haben, sich gegen gesellschaftliche Widerstände durchzusetzen. Er hat noch nie gehört oder will es nicht wahr haben, dass der Staat gerade Freiräume sichert, dass er die schwächeren Individuen gegen die stärkeren schützt und eben deswegen selbst nicht weiter geschwächt werden darf. Die einfache Erkenntnis, dass der Einzelne immer mit anderen Individuen, Gruppen und Organisationen zusammenlebt, von denen er seinerseits teils gefördert, teils behindert, immer aber beeinflusst wird, fehlt in der simplen Weltanschauung dieses Abgeordneten, der als Softwareentwickler erfolgreich sein mag, aber offensichtlich von sozialen und politischen Zusammenhängen nichts weiß. Es ist wahrlich befremdend, dass ein Mensch des Jahrgangs 1965 die längst überholte altliberale Entgegensetzung von „Mensch" und „Staat" wieder aufleben lässt. Wie falsch diese Front ist, zeigt neuestens wieder der bittere Kampf um Steuern und Sozialleistungen in den USA, wo es den radikalen Staatsfeinden immer noch gelingt, Staat und Verwaltung zu diffamieren und die Kluft zwischen Arm und Reich immer weiter zu vergrößern.

Voraussetzungen funktionierender Demokratie

Direkte und indirekte Volksvertretung

Die repräsentative Demokratie leistet mehr als ihre Kritiker ihr zubilligen. Sie ist die Organisationsform der verbindlichen Willensbildung des Volkes und begründet überhaupt erst die Handlungsfähigkeit der gemeinsamen Ordnung. Ohne Repräsentation gibt es gar keine Gemeinsamkeit des Willens und Handelns. Auch die Qualität der repräsentativ getroffenen Entscheidungen ist meist viel besser als gemeinhin behauptet wird; die Enttäuschungen der Bürger beruhen zum größeren Teil auf den Interessengegensätzen und anderen nicht überwindbaren Schwierigkeiten der zu regelnden Materien. Unser parlamentarisches Regierungssystem ist

206 Pavel Mayer 2011.

eine höchst effektive Organisation zur Bündelung und Filterung von Interessen. Entgegen der Meinung vieler Kritiker ist das Parlament auch bei der Gesetzgebung durchaus aktiv und nickt keineswegs nur die Vorschläge der Regierung ab. Mit Recht wird gesagt: Kein Gesetz verlässt den Bundestag so, wie es (als Regierungsentwurf) hineingekommen ist.

Trotzdem ist es angebracht, dass zu den repräsentativen, also indirekten Formen der Demokratie solche der unmittelbaren Teilhabe des Volkes an den politischen Entscheidungen treten. In allen Ländern der Bundesrepublik sind seit 1990 die Verfassungen geändert worden, um diesem Interesse Rechnung zu tragen: Überall kann ein Verfahren in Gang gesetzt werden, an dessen Ende ein verbindlicher Volksentscheid steht. Auf Bundesebene fehlt diese Möglichkeit noch, obwohl gerade dort die meisten wichtigen Entscheidungen getroffen werden; denn der Bund hat umfassende Gesetzgebungsbefugnisse auf den meisten Gebieten des Soziallebens.

Über die Modalitäten der unmittelbaren Volkswillensbildung ist schon viel gestritten worden. Radikale Vertreter der direkten Demokratie verlangen, dass Volksentscheide auch ohne Erreichen eines bestimmten Quorums der Abstimmenden oder Abstimmungsberechtigten verbindlich seien. Das gilt in der Schweiz tatsächlich so. In unserer ganz anders gearteten politischen Ordnung wäre der Verzicht auf jegliches Quorum nicht vertretbar. Wenn nicht eine Mindestzahl von Bürgern – errechnet als Anteil an den Abstimmungsbefugten – sich an der jeweiligen Abstimmung beteiligt oder dem Volksbegehren zugestimmt hat, kann der Volksentscheid nicht verbindlich sein. Es ist nicht überzeugend, dass eine kleine Minderheit die Entscheidung des Parlaments ersetzen soll, und der zugrunde liegende Streit kann auf diese Weise nicht befriedet werden.

Ohnehin ist die Anrufung des Volkes immer mit der Möglichkeit verbunden, dass eine gut organisierte und finanzstarke *Minderheit* ihre Interessen gegen die weniger artikulationsfähige Mehrheit durchsetzt. Gut betuchte, klug vorgehende Mitbürger in den besseren Wohnvierteln haben in Hamburg durch Volksentscheid eine Schulreform verhindert, die den Schülern in schlechteren Verhältnissen zugutegekommen wäre, nämlich das gemeinsame Lernen bis zur sechsten Klasse. Man kann das Ziel für richtig halten und sich mit dem Volksentscheid abfinden – er hat übrigens das vorgeschriebene Quorum deutlich überschritten; die Befürworter hatten gut organisiert – aber niemand sollte sagen, die Entscheidung sei sozial ausgeglichen.

Es widerspricht aller Erfahrung, den Erzeugnissen der direkten Demokratie generell eine *höhere Qualität* als den Parlamentsgesetzen und Regierungsmaßnahmen zuzubilligen; dazu sind sie viel zu umstritten, manchmal sogar mit Grundrechten, Minderheitenschutz oder rechtsstaatlichen Prinzipien unvereinbar. Sofern man den unmittelbaren Äußerungen des Volkes einen höheren rechtlichen Rang

einräumen möchte – etwa indem man die nachträgliche Änderung oder Aufhebung von Volksgesetzen verfassungsrechtlich verbietet oder erschwert[207] – , geschieht dies nicht etwa, weil man glaubte, sie seien immer höherwertig. Vielmehr hält man es für *angemessen*, dass der nicht durch Vertreter vermittelte Volkswille sich durchsetzt, die Menschen also in höherem Maße „sich selbst gehorchen" als im Falle ihrer Repräsentation durch das Parlament. Hier wirkt Rousseaus „Identitätslehre" nach: Die Meinung des Volkes soll nicht durch Zwischeninstanzen verfälscht werden. Heute bestreitet jedoch niemand mehr, dass diese Lehre allenfalls in Dörfern, Kleinstädten und kleinen Landgemeinden wie dem Kanton Appenzell Innerrhoden funktioniert – und auch das nur, weil es auch dort überall Repräsentanten, Organisatoren und Mediatoren gibt. Die Vorstellung der „volonté genérale", die sich auf geheimnisvolle Weise unmittelbar zwischen Individuum und Staat herausbildet, ist in einer Massendemokratie nicht nachvollziehbar. Sie ist überdies zumindest in Deutschland durch historische Exzesse der Akklamationsdemokratie – man denke an Reichsparteitage, einen „gesäuberten" Reichstag und frenetisch bejubelte Sportpalast-Reden – längst diskreditiert.

Nun wird behauptet, man könne die unmittelbare Beteiligung der großen Menge der Bürger im Internet so einrichten, dass die einzelne Stimme mehr Gewicht erhält als wenn sie sich im Chaos der Offline-Öffentlichkeit behaupten müsste. Das Internet wäre dann so etwas wie die technische Umsetzung von Rousseaus Utopie einer unverfälschten Selbstbestimmung des Volkes. Man möchte dieses schöne Bild gern für realisierbar halten, und es ist ja richtig, dass mittels der Technik viel *mehr* Menschen sich in kürzester Zeit zu politischen Sachfragen äußern können als über andere Medien. Wenn Gruppen von Aktiven oder Interessenten im Netz zu Stellungnahmen auffordern, kommen schnell Hunderttausende, ja Millionen von Zustimmungen zustande. Eine kleine Schar von Hauptamtlichen kann unter günstigen Umständen große Teile der Weltbevölkerung zu den nötigen Klicks veranlassen, die sich zu eindrucksvollen Manifestationen bündeln lassen – gegen Unterdrückung und Rassismus, gegen den Raubbau an der Umwelt, gegen soziale Ungleichheit und politische Willkür usw. usw. So rühmen sich die Internet-Aktivisten der Organisation „Avaaz" mit berechtigtem Stolz, dass sie „mehrere hundert Kampagnen durchgeführt und eine wichtige Rolle bei Dutzenden Erfolgen gespielt haben", u.a. indem sie „die Pläne von Rupert Murdoch zur Dominierung der Weltmedien durchkreuzt", „die Mediensperre in Syrien durchbrochen und die mutigen Demokratiebewegungen im Mittleren Osten unterstützt", „Ugandas Entwurf zur Einführung der Todesstrafe für Homosexualität blockiert" und „den Bau einer Schnellstraße durch geschützte indigene Gebiete in Bolivien aufgehalten" ha-

207 So geschehen in der Hamburger Verfassung Art. 50 Absatz 4.

ben.[208] Das sind wichtige Ziele und schöne Erfolge, an denen freilich jeweils auch viele andere – vor allem auch offline – beteiligt waren.

Die Resolutionen und Petitionen, die bei solchen Initiativen herauskommen – seien sie national, seien sie übernational organisiert –, verändern nicht automatisch die Welt. Sie überzeugen verantwortliche Politiker, die bisher andere Wege gehen wollten, sie bilden ein Ventil für Überdruck im politischen Zustand ganzer Völker und haben manchmal durchschlagenden Erfolg gegenüber Partikularinteressen, die bisher durch Lobbyarbeit abgesichert waren. Aber den Resultaten geregelter, regelmäßig stattfindender politischer Entscheidungsprozesse (und Wahlen!) können sie nicht gleichgestellt werden. Sie sind ebenso das Ergebnis funktionierender Organisation wie die Äußerungen der Gegenseite; ihnen fehlt jedoch die Repräsentativität selbst dann, wenn sie riesige Zustimmungsquoten erreichen, und harte Kontrahenten setzen sich darüber hinweg.

Freunde des Internet werben mit der Behauptung, im Netz könne jeder seine Interessen selbst vertreten. Das ist richtig, soweit „vertreten" schlicht als „*äußern*" verstanden wird. Aber wie wird die Botschaft *empfangen*? Zunächst als zu speichernde Nachricht auf einem Computer. Eigene Interessen im Netz zu „vertreten", bedeutet also zunächst nur eine potentiell größere *Verbreitung* der eigenen Ansichten und Forderungen. Erfolgreiche Interessenvertretung setzt aber trotz aller Verbreitung voraus, dass andere sich des Anliegens annehmen. Eine Initiative aus dem unorganisierten Volk heraus wird überhaupt nur wahrgenommen, wenn jemand sie „vertritt". Auch die direkte Demokratie bedarf auf allen Ebenen der Repräsentation! Manchmal sind es bekannte Persönlichkeiten, die als offizielle Vertrauenspersonen einer Volksinitiative auftreten, manchmal Hinterzimmer-Aktivisten einer kleinen Gruppe, die aus Eigeninteresse oder um des Gemeinwohls willen, so wie sie es verstehen, eine große Menge anderer zum Mitmachen bewegen, und bisweilen sogar parteipolitisch Aktive, die auf dem Weg über die Volksbeteiligung die Widerstände umgehen, die ihnen im parlamentarischen Prozess entgegentreten.

Für den Erfolg der Internet-Demokratie ist – nicht anders als in der Offline-Politik – entscheidend, wie die Empfänger mit der Botschaft umgehen.[209] Wenn viele gleichgerichtete Petitionen oder Initiativen eingehen, kann das die Betreiber beeindrucken, muss aber nicht. Vielleicht reagieren die Empfänger wirklich in dem gewünschten Sinne, aber vielleicht auch gerade nicht. Wenn die geäußerten Interessen mit denen der Mächtigen kollidieren, setzen sie sich nicht ohne weiteres durch, sondern provozieren Abwehrreaktionen. Im schrecklichsten Fall setzen die Machthaber gegen die opponierenden Menschen Gewalt ein. Auf jeden Fall werden sie erforschen, ob die vielen Absender tatsächlich eine Mehrheit des Volkes dar-

208 Rundmail vom 6.1.2012.
209 Zur Kritik der Internet-Demokratie: Jun 2009.

stellen. „Im Internet weiß niemand genau, wer hinter den vielen steckt. Und wie viele diese vermeintlich vielen wirklich sind“[210].

Die schöne Vorstellung, dass sich aus den vielen individuellen Äußerungen im Netz eine einheitliche (oder zumindest eine deutlich von der Mehrheit getragene) Richtung herauskristallisiert, ist so realistisch wie das Vertrauen auf die „unsichtbare Hand“ des Marktes, der nach liberaler Ansicht das Gemeinwohl hervorbringt. Das Volk besteht aber nicht nur aus Idealisten, die das Beste für die Allgemeinheit wollen, sondern aus vielen (oft sehr liebenswürdigen) Egoisten, die sich selbst mehr als die Nächsten lieben. An der Bildung der öffentlichen Meinung und der politischen Entscheidungen nehmen einerseits keineswegs alle Bürger teil,[211] andererseits wirken außer Individuen alle möglichen Vereinigungen und Verbände, Unternehmen, Parteien und Gruppen mit. Wenn es keine verbindlichen Verfahrensregeln gibt und die Abstimmungsbefugnis nicht kontrolliert wird, kann aus der Vielfalt der Meinungsbekundungen keine „demokratische“ Entscheidung hervorgehen, weil eben der Demos nicht angemessen repräsentiert ist.

„Das Volk“ ist keine Einheit, die man sich als eine unstrukturierte Menge natürlicher Personen vorstellen könnte. Es ist eine verfassungsrechtliche Idee, ein politisches Konstrukt, und es setzt sich ganz unterschiedlich zusammen, je nachdem in welchem Kontext man von ihm spricht. Es braucht nicht einmal die zahlenmäßige Mehrheit der Bevölkerung zu sein; nach den Regeln der Verfassung ist „Volk“ die Gesamtheit der Personen, die an einer Wahl oder Abstimmung teilnehmen dürfen; diese Gesamtheit ist der „Träger der Staatsgewalt“ im Sinne des Grundgesetzes. Welche Meinung und welche Entscheidung dem deutschen Volk (im Rechtssinne) zugeschrieben wird, das entscheidet die *Mehrheit* in dem jeweiligen rechtlich geregelten Verfahren.

„Wir sind das Volk“, der wirkmächtige Slogan der friedlichen Revolution in der DDR, war keine verfassungsrechtliche Aussage, sondern Ausdruck des Selbstgefühls der Montagsdemonstranten, die sich für die Gesamtheit verantwortlich fühlten. Damals hat die kleinere, mutigere Hälfte der DDR-Bürger sich durchgesetzt. Nur ist das kein Beispiel für das Volkshandeln in einer konsolidierten Verfassungsordnung, sondern für einen revolutionären Vorgang.

Auch die Stuttgarter Bahnhofsgegner empfanden sich bis zur Volksabstimmung am 27. Oktober 2011 als die engagierte Mehrheit des Landesvolks; sie hielten sich für die besseren Demokraten als die Befürworter des unterirdischen Bahnhofs und als diejenigen, denen das Thema egal war. In der förmlichen Abstimmung aber artikulierte sich – nach den in der Landesverfassung vorgeschriebenen Regeln –

210 Borchardt 2011.

211 Daten hierzu bei Emmer/Vowe/Wolling 2011, insbes. S. 225 ff. (typologische Längsschnittanalyse von Angelika Fütting). Danach ist etwa die Hälfte der Bevölkerung politisch desinteressiert („passive Mainstreamer“, die generell politische Aktivitäten meiden). S.a. Voss 2012.

der in dieser Frage verbindliche Wille des Landes-„Volkes“. Auch hier spielte übrigens das Problem eine Rolle, wie das zur Entscheidung berufene „Volk“ abzugrenzen sei: nur die Bürger in der Region Stuttgart, die von dem Bahnhofsumbau besonders betroffen sind, oder – wie es die Verfassung gebot – alle Bürger des Landes Baden-Württemberg oder gar alle Bundesbürger (weil die Bahn überregionale Bedeutung hat und vom Bund getragen wird)?

Die Bedenken gegen ungeregelte Partizipation gelten schon bei Offline-Abstimmungen; für die Online-Demokratie sind klare Regeln erst recht notwendig. Nicht nur die Manipulationsmöglichkeit, die im Netz groß ist, muss zur Vorsicht mahnen. Die Internet-Abstimmung ist leicht zu organisieren – zu leicht, um davon die politische Entwicklung des Gemeinwesens abhängig zu machen. Es fehlt die Notwendigkeit, sich zum Abstimmungslokal zu begeben oder wenigstens einen Abstimmungsbrief abzuschicken. Das empfinden zwar manche als einen Vorteil und halten die „physische“ Beteiligung an Wahlen und Abstimmungen für zu beschwerlich oder gar unzumutbar. Sie übersehen, dass diese kleinen Hürden systemimmanent und sinnvoll sind.

Demokratie braucht Zeit

Benjamin R. Barber, einer der bekanntesten amerikanischen Politikwissenschaftler, hat sich intensiv mit der „elektronischen Demokratie“ befasst. Er betont, dass das Überleben und das Gedeihen der Demokratie „nicht von der Qualität und dem Charakter unserer Technik“ abhängt, sondern „von der Qualität unserer politischen Institutionen und dem Charakter unserer Bürger“.[212] Deshalb sind „unsere ersten Fragen – wie es immer war – nicht technische, sondern politische“.[213] Und in einem früheren Artikel hat Barber sein Demokratieverständnis so erläutert:

> „Demokratie baut auf Besonnenheit, Umsicht, Interaktionen im Schritttempo und zeitraubende (folglich ‚ineffiziente‘) Formen multilateraler Konversationen, die nach postmodernen Maßstäben schwerfällig sind, einem viel Zeit abverlangen, einige Anforderungen stellen, die nicht terminierbar sind und so gut wie nie unterhaltsam genannt werden können. […] Demokratie ist so langsam wie das abwägende Urteilen, das sich in der Tat nicht gerade schnell vollzieht; sie verlangt ebenso nach Stillschweigen wie nach dem kommunikativen Austausch und macht es gelegentlich erforderlich, dass Tage oder Monate verge-

212 Barber 2009, S. 217. Um die Bewahrung der politischen Kultur, zu der gerade auch ein angemessener Stil der politischen Kommunikation gehört, sorgen sich auch kritische Stimmen in der Auseinandersetzung mit der Piratenpartei ab, z. B. Stephan 2012 und Zielcke 2012.

213 Barber 2009, S. 217, frei übersetzt.

hen müssen, ehe weitere Überlegungen angestellt oder weitere Schritte eingefordert werden können".[214]

Das ist so aktuell wie je: Demokratie braucht Zeit, aber das Internet ist schnell, zu schnell für die Demokratie. Diese funktioniert nicht, wenn die Entscheidungen – z.B. die Auswahl der Repräsentanten oder ein Gesetzesbeschluss – spontan, unüberlegt, ohne Anhörung von Argumenten zustande kommen. Es klingt verlockend, das Volk laufend an politischen Beratungen zu beteiligen, aber es wäre eine miserable Form von Volksbeteiligung, wenn alle ständig – online oder sonstwie – abstimmen müssten, nämlich Stimmungsdemokratie ohne inhaltliche Substanz. Unverzichtbare Voraussetzung qualifizierter demokratischer Politik ist der öffentliche Austausch von Argumenten und Beweisen. Demokratie braucht Zeit zum Überlegen, zum Austragen von Streitigkeiten, zur Erarbeitung akzeptanzfähiger Lösungen. Damit durchdacht entschieden wird, braucht es Entschleunigung, nicht weitere Beschleunigung. Demokratie braucht auch Raum im ganz einfachen Sinne: Parlamente, in denen wir die Abgeordneten bei der Arbeit sehen können, Kongresshallen, Vereinslokale, Parteihäuser, in denen Menschen sich versammeln, um unmittelbar miteinander zu kommunizieren. Wenn die Mitglieder der Piraten-Partei in ihren Versammlungen auf die Laptops blicken, statt sich gegenseitig zuzuhören, vergessen sie ihre eigentliche kommunikative Aufgabe. Sie tun dies, damit andere ihnen über die Schulter schauen und sie kontrollieren können – ein lobenswerter Vorsatz, aber im Ergebnis bieten sie ihren Zuschauern ein groteskes Zerrbild von demokratischer Beratung.

Auch der viel geschmähte Wahlkampf, die öffentliche mediale oder unmittelbare Auseinandersetzung über Ziele und Mittel der Politik ist eine unverzichtbare Voraussetzung demokratischer Willensbildung. Menschen, die sich für fortschrittlich halten, mögen Wahlversammlungen und Straßenstände der Parteien meiden und sich lieber am häuslichen PC oder Fernseher informieren, aber wenn alle das täten, bräuchten wir uns nicht über den Niedergang des politischen Systems zu wundern.

Blitzumfragen und andere demoskopische Schnellschüsse zu einzelnen Sachfragen oder zur Beliebtheit von Personen und Parteien beleben das politische Alltagsgeschäft, warnen die Repräsentanten vor Überheblichkeit und setzen bisweilen langfristige Änderungen der öffentlichen Meinung in Gang. Aber sie dürfen nicht verbindlich sein. Es ist schlimm genug, dass sich Regierungen und Parlamente an punktuellen Meinungsbildern orientieren, die aus Umfragen hochgerechnet worden sind; dieses Schielen nach der jeweiligen Mehrheitsstimmung ist mit der Grundpflicht der Abgeordneten unvereinbar, sich eine unabhängige Meinung zu

214 Barber 1998, S. 5. S. a. Bull 1999.

bilden. Auf keinen Fall darf die Express-Bürgerbeteiligung zum Ideal verklärt werden.

Der Austausch, den politisch Engagierte im Netz pflegen, hat einen ganz anderen Charakter als die Face-to-face-Kommunikation in öffentlichen Versammlungen, Kneipenrunden oder Kollegengesprächen. Nur selten wird wirklich diskutiert; oft fehlen Argumente und Beispiele, oft schon der Wille, andere zu überzeugen. Viele Internet-Foren sind Ansammlungen übler gegenseitiger Beschimpfungen. Vorurteile und Mäkeleien prägen den Stil, Fairness und Toleranz sind Ausnahmeerscheinungen. Die Anonymität, die das Netz bietet, nimmt offenbar manchen Bloggern jegliche Scheu. Sie lassen Wut und Hass heraus, und die Attackierten können sich nicht wehren; ebenso wenig sind Sanktionen von Arbeitgebern oder Behörden zu erwarten. Aber der Gefühlsmüll, der auf diese Weise abgeladen wird, vergiftet die Atmosphäre; für ernsthafte Diskussionen wird das Netz dadurch uninteressant und am Ende vermutlich irrelevant.

Dass Volksabstimmungen umsichtig vorbereitet und geregelt sein müssen, hat jüngst ein Vorgang in Hamburg eindrucksvoll belegt, der nach dem Wunsch seiner Urheber einen Durchbruch direkter Demokratie auf einem davon bisher unberührten Gebiet bringen sollte. Das Thalia Theater ließ seine Zuschauer und Freunde brieflich und elektronisch über den Spielplan für das Jahr 2012 abstimmen, ohne hinreichende Vorgaben zu machen und die Prozeduren gegen Missbrauch abzusichern. Das Ergebnis war – bei recht geringer Beteiligung – nach Ansicht von Kritikern „komplett sinnlos“[215]. Offensichtlich hatten sich Gruppen interessierter Teilnehmer einen Spaß daraus gemacht, mit E-Mails, Facebook-Eintragungen usw. bestimmte Stücke massenhaft zu unterstützen. Man darf vermuten, dass auch Freunde und Sympathisanten bestimmter Autoren auf diesem Wege Einfluss ausüben wollten. Nun sind die Initiatoren blamiert, und die Zeitungen schreiben, dass Demokratie im Theater nichts zu suchen habe; Dramaturgen und Intendanten sollten ihre Aufgabe, den Spielplan zu gestalten, selbst erledigen, und die Abstimmung finde schließlich an der Kasse statt. „Netz-Voting in seiner wesenshaften Willkür verhält sich zu seriöser Demokratie wie Exorzismus zu Biologie“[216].

Elektronische Wahlen und alltägliche „Verflüssigung” der Demokratie?

Ein vergleichsweise einfaches Thema ist es, ob und wie demokratische Wahlen mit Hilfe elektronischer Geräte oder sogar über das Internet durchgeführt werden können.[217] Man verspricht sich davon insbesondere, dass mehr Wahlberechtigte, denen

215 So Briegleb 2011.
216 Briegleb 2011.
217 Auch dazu Beiträge in dem Sammelband von Holznagel/Grünwald/Hanßmann 2001.

der Gang zum Wahllokal schwer fällt – z.B. alte und behinderte Menschen – ihr Beteiligungsrecht wahrnehmen werden. Für die Technikfans ist „E-democracy" eine einfache Sache: Wahlen und Abstimmungen müssen so organisiert werden, dass die Voten der Bürger richtig gezählt und zugeordnet werden, das Verfahren also gegen Manipulationen gesichert ist und dass die Einhaltung der Wahlgrundsätze gewährleistet ist: Wahlen müssen allgemein, unmittelbar, frei, gleich und geheim sein (wie es z.B. Art. 38 Grundgesetz vorschreibt). Diese Bedingungen sollen mit Hilfe elektronischer Signaturen oder auf andere Weise erfüllt werden, und so ist dann für einen Datenverarbeiter die „wichtigste Voraussetzung für die intensive Netznutzung", „dass die Zahl der Inhaber von elektronischen Signaturen in der Bundesrepublik zunimmt".[218] Nachdem die elektronische Signatur sich nun aber in den letzten zehn Jahren keineswegs durchgesetzt hat, müssten wohl andere Überlegungen angestellt werden.

Mehrfach ist – als eine Vorstufe zu Internet-Wahlen – die Einführung von Wahlmaschinen versucht worden, aber die Geräte wurden meist als zu unzuverlässig oder intransparent eingeschätzt. „Alle wesentlichen Schritte der Wahl" müssen „öffentlicher Überprüfbarkeit unterliegen" – so hat das Bundesverfassungsgericht im März 2009 in einem Grundsatzurteil entschieden, und weil es daran haperte, hat es festgestellt, dass die Verwendung der elektronischen Wahlgeräte einer niederländischen Firma bei den Wahlen zum 16. Deutschen Bundestag (2005) verfassungswidrig war. Solche Geräte dürfen nur zugelassen werden, wenn „eine dem verfassungsrechtlichen Grundsatz der Öffentlichkeit der Wahl entsprechende Kontrolle" sichergestellt ist.[219] Der Wähler muss „zuverlässig nachvollziehen" können, „ob seine Stimme unverfälscht erfasst und in die Ermittlung des Wahlergebnisses einbezogen wird und wie die insgesamt abgegebenen Stimmen zugeordnet und gezählt werden".[220] Die Bundeswahlgeräteverordnung habe das nicht garantiert, und bei den zu beurteilenden Geräten sei das nicht möglich gewesen.[221]

Mit einem ganz anderen Versuch, die Wahlen technisch zu vereinfachen, ist vor einigen Jahren die Hamburger Bürgerschaft gescheitert. Sie hatte im Frühjahr 2006 den Einsatz des „digitalen Wahlstifts" bei der Bürgerschaftswahl im Februar 2008 beschlossen. Dabei handelt es sich um ein Gerät, mit dessen Hilfe die Wähler ihre Stimmen auf besonders präpariertem Papier ankreuzen und eine eingebaute Minikamera die Position (also die gewählte Partei oder den gewählten Kandidaten) dokumentiert. Die Auswertung wäre erheblich erleichtert worden, was bei dem neuen, sehr komplizierten Hamburger Wahlsystem eine große Erleichterung bedeutet hätte. 12.000 solcher elektronischer Wahlstifte wurden bestellt. Dann aber kam Kritik

218 Rüß 2001, S. 521. Der Autor ist Dezernent im Landesbetrieb für Datenverarbeitung und Statistik, Brandenburg.
219 Urteil des BVerfG v. 3. 3. 2009, BVerfGE 123, 39-88.
220 Ebd. S. 70.
221 Ebd. S. 82 ff. und 85 ff.

aus den Reihen der Grünen auf, und bei einer Expertenanhörung im November 2007 demonstrierte der Chaos Computer Club, dass das Papier der Stimmzettel manipulierbar sei. Die Technik der Auszählung und Zuordnung der Stimmen wurde nicht beanstandet, aber ein Unbehagen an der Undurchsichtigkeit der Technik dürfte ebenfalls eine Rolle gespielt haben. Jedenfalls wurde das Unternehmen aus Furcht vor Wahlanfechtungen abgebrochen, die Wahlstifte blieben unbenutzt, und die Wahlhelfer hatten tagelang zu tun, die Ergebnisse festzustellen.

Wahrscheinlich war die Angst vor Manipulationen vollkommen unbegründet; die Vorbereitungen fanden ja unter mehrfacher Kontrolle der streng verpflichteten Wahlleiter und Wahlhelfer statt. Aber es fehlte das nötige Vertrauen in die Technik und die sie benutzenden Personen.

Als eine „Mischform zwischen direkter und indirekter Demokratie" empfehlen die Piratenpartei und ihre Trabanten die „Liquid Democracy". Die „flüssige" Demokratie mit dem „fließenden Übergang" zwischen Repräsentation und direkter Beteiligung soll eine basisdemokratische Alternative zum System der Vertreterversammlungen darstellen, wie es sonst in allen Parteien besteht, deren Mitglieder sich nicht mehr an einem Ort versammeln können. Dahinter steht freilich eine grundsätzliche Absage an jede Form der Vertretung: Jedes Mitglied (und vielleicht sogar jeder, der es will) soll „zu jeder Zeit gezielt zu einzelnen Themen verbindlich Stellung beziehen" können.[222] Zunächst wird dieses Verfahren zur Stärkung der innerparteilichen Demokratie eingesetzt – übrigens in einer eigenen Variante auch von der SPD – , aber das Ziel der Piratenpartei ist offenbar, es auch auf Sachentscheidungen durch das Volk anzuwenden – damit die Menschen nicht nur alle vier oder fünf Jahre wählen können. Ein „Tool" zur Direkt-Äußerung vieler, das von verschiedenen Organisationen (einschließlich der Bundestags-Enquetekommission „Internet und digitale Gesellschaft") benutzt wird, hat den sinnigen Namen „Adhocracy": Herrschaft der ad-hoc-Abstimmenden.

Überwunden werden soll auf diese Weise auch die Bündelung der politischen Themen und Programmpunkte durch die politischen Parteien. Dazu soll ein System des „delegated voting" dienen, genauer der Möglichkeit, dass der einzelne Wähler seine Stimme entweder selbst abgibt oder sie einer Partei oder einem Einzelnen überträgt:

> „Jeder Teilnehmer kann zu jedem Zeitpunkt für sich selbst entscheiden, wo auf dem Kontinuum zwischen repräsentativer und direkter Demokratie er sich aufhalten möchte", zum Beispiel: „Für Steuerrecht möchte ich gern durch die Partei SPD, für Umweltpolitik durch die Partei Die Grünen und für die Schulpolitik durch die Privatperson Herrn Müller vertreten werden. Für die Ent-

222 So die Internetseite der Piratenpartei zu „Liquid Democracy". Dort auch die weiteren Zitate.

scheidung über das neue Hochschulzulassungsgesetz möchte ich aber selbst abstimmen."

Das klingt verführerisch. Die erwarteten Einwände,[223] dadurch würde die Politik unberechenbar und wetterwendisch, weisen die Piraten zurück; selbstverständlich seien die so gefassten Beschlüsse – je nach Themenkreis – in bestimmter Weise verbindlich (etwa: das Wahlprogramm sei eben für die bevorstehende Wahl verbindlich), und es sei auch nicht verkehrt, bei Änderung der Verhältnisse die früheren Beschlüsse wieder aufzuheben oder zu ändern. Dass ein solches Demokratieverständnis die politischen Parteien durcheinander wirbeln und letztlich wohl zerstören werde, dürfte den Fundamental-Oppositionellen ganz recht sein. Sie halten ohnehin nichts von den etablierten Parteien und fühlen sich als Avantgarde, die ein ganz neues Demokratieerlebnis herbeisehnen. Dass man auf diese Weise auch den Parlamentarismus abschaffen kann, ist ihnen vielleicht nicht bewusst. Jedenfalls glauben sie an die Realisierbarkeit dieses Verfahrens und damit an die Kreativität derer, die darin den Ton angeben.

Es läge den Piraten vermutlich sehr fern, sich in diesem Zusammenhang selbst als Repräsentanten des Volkes zu erkennen – aber nichts anderes wären sie und all die anderen, die mittels dieses Instruments staatliche Führungspositionen erlangen. Es fände ein Austausch der politischen Elite statt, der (zumindest auf längere Zeit, aber möglicherweise dauerhaft) mit einer weitgehenden Intransparenz und Instabilität der Machtverhältnisse verbunden wäre. Und diese neue Verfassung hätte einen schweren Geburtsfehler, den die Protagonisten der direkten Demokratie oft übersehen: Sie würde ohne Not auf die enorme Leistungsfähigkeit des Parlaments als Problemlöser verzichten. Auch dieser Traum von mehr Demokratie würde vermutlich mit vielen Enttäuschungen enden – Enttäuschungen über unerwartete Ergebnisse wie das Ende der Schulreform in Hamburg oder das Minarettverbot in der Schweiz.

Fazit: Die Fortentwicklung der Demokratie und des parlamentarischen Regierungssystems ist kein Spiel. Sie fordert gründlichere Bemühungen und realistischere Überlegungen als das Ausprobieren komplizierter Abstimmungsmethoden.

Bessere Politik durch mehr Technik – ein schöner Traum

Wer Selbstbestimmung und Partizipation nicht schon als Selbstzweck ansieht, sollte immerhin fragen, ob selbstbestimmte Entscheidungen höheren Wert haben, ob Teilhabe zu höherer Akzeptanz führt? Es gehört jedenfalls auch zur Werbung für das Internet, dass durch Teilhabe der Betroffenen eine „bessere" Politik möglich

223 Vgl. dazu Seckelmann/Bauer 2012, S. 327 ff. (334 ff.).

werde. Andere denken daran, dass mehr Sachverstand in die Entscheidungsprozesse einbezogen werden kann, wenn die Entscheidungsträger sich des Netzes bedienen.

Dass wir nicht naiv auf die bessere Qualität der direkt-demokratischen Willensbildung setzen können, habe ich schon dargelegt. *Quantitativ* hat die Beteiligung an der Bildung der öffentlichen Meinung zugenommen, und das Netz ist dabei ohne Frage das erfolgreichste Medium; die Steigerung der Beteiligungsquote ist beeindruckend. Setzt man diese Zunahme des Interesses aber in Beziehung zu der Zunahme der Internetnutzung insgesamt, wird die Aussage deutlich relativiert: Wenn so viel mehr Menschen täglich im Internet surfen, ist die vermehrte Teilnahme an politischen Meinungsbekundungen nicht mehr überwältigend. Die Adressaten werden dieses Verhältnis genau beobachten und ihre Schlüsse daraus ziehen.

Wenn alles gut geht, nutzen wir das Internet künftig so, dass mehr Menschen intensiver an der gemeinsamen Macht teilhaben. Herrschaftswissen wird in geringerem Maße bei Insidern liegen; Regierende müssen sich stärker der Nachfrage und der Kritik aus dem Volk stellen. Das Internet wird auch vielen dazu helfen, die Welt besser zu verstehen und sich umfassender als bisher zu bilden. Aber was können wir tun, um dorthin zu gelangen? Dass wir das Netz gezielt – durch staatliche Maßnahmen, also Gesetze oder Einzelanordnungen – zur Stärkung der Demokratie aktivieren können, erscheint mir unwahrscheinlich. Das Internet ist keine weltweite Zentrale für politische Bildung. Wir wollen und können dem Staat nicht die Entscheidungsbefugnis dafür einräumen, was über das Netz verbreitet werden darf; das wäre Zensur, wie wir sie gerade überwunden haben.

Die heikelste Aufgabe in Sachen „Demokratiepflege“ besteht darin, die Verfahrensweisen der Internet-Partizipation so zu gestalten, dass zwar ein Höchstmaß an Bürgerbeteiligung möglich wird, der Volkswille aber nicht zugunsten von Minderheiten verzerrt wird. Nicht nur das Parlament, sondern auch die einzelne Sachinitiative muss, wenn sie von der Gesamtheit akzeptiert werden soll, „repräsentativ“ sein oder genauer: auf Repräsentativität abzielen. Wer verbindliche Volksentscheide oder (auf kommunaler Ebene) Bürgerentscheide will, muss deshalb bedenken, dass es finanzstarken, gut organisierten oder gut vernetzten Gruppen relativ leicht fällt, eine große Zahl von Unterstützern für ihre Anliegen zu gewinnen, auch wenn vielleicht die Mehrheit der Betroffenen dagegen ist. Diese Fehlentwicklung kann dadurch abgeschwächt werden, dass ein Volks- oder Bürgerentscheid nur verbindlich ist, wenn ein bestimmter Teil der Abstimmungsberechtigten dafür votiert hat bzw. an der Abstimmung teilgenommen hat. So sind Beteiligungs- oder Zustimmungsquoren in den meisten deutschen Landesverfassungen und Gemeindeordnungen vorgeschrieben. Diese „Quoren“ schwanken zwi-

schen fünfundzwanzig und (bei Verfassungsänderungen durch Volksentscheid) fünfzig Prozent.[224]

Die Protagonisten der direkten Demokratie halten dem – salopp gesagt – entgegen, dass die Mehrheit „selbst schuld" sei, wenn sie von ihrem Beteiligungsrecht keinen Gebrauch macht; die Gegner könnten, darauf spekulierend, durch den Aufruf zur Nichtbeteiligung jedes noch so gute Anliegen kaputt machen. Aber es ist durchaus angebracht, für die Abstimmung des Volkes über einzelne Sachthemen, die sonst im Parlament beraten werden, gewisse – aber nicht zu hohe – Hürden vorzusehen; denn die Initiativen, die das Volk unmittelbar anrufen, sind vor der Korruption durch Eigeninteressen ebenso wenig gefeit wie die gewählten Abgeordneten.

Auf jeden Fall müssen die Partizipationsverfahren klar und transparent geregelt sein. Die Teilnehmer müssen gleich behandelt werden, und sie müssen wissen, was aus ihrer Abstimmung folgen kann. An bestimmten Stellen des Abstimmungsprozesses müssen die Stimmen gezählt und die Ergebnisse festgestellt werden, und diese müssen wenigstens für einige Zeit Bestand haben. Wenn über denselben Gegenstand in kurzem Abstand erneut abgestimmt wird, kommen kurzfristige Stimmungsschwankungen zutage, und die gründliche Erarbeitung nachhaltiger Lösungen wird unmöglich. (Schon die parlamentarischen Legislaturperioden von vier oder fünf Jahren sind zu kurz für langfristige Planungen, und genau das ist ein wesentlicher Grund für viele Fehlentwicklungen – vom Umweltschutz bis zur Finanzkrise). Die Methode der „Liquid Democracy" führt zwingend dazu, dass noch kurzfristigere und damit noch weniger nachhaltige Entscheidungen produziert werden. Das mag für die innerparteiliche Willensbildung der „Piraten" gerade noch angehen; für die Bildung des Volkswillens insgesamt wäre sie Gift.

Was die Teilnahme von Sachverständigen an dem politischen Diskurs angeht, so ist auch sie gestiegen – und ist ebenfalls zu relativieren. Es verwundert nicht, dass auch der Glaube an die Experten durch die Ausbreitung der weltweiten Netzkommunikation zugenommen hat, aber dieser Glaube ist seinerseits keine tragfähige Basis für eine vollkommene Demokratie der Zukunft. Technisch perfektionierte Wissensgenerierung und Sachverstandsbeteiligung führen eben nicht von selbst zu besseren Entscheidungen.

Zwar müssen wir unbedingt daran festhalten, dass der politische Wille der Gemeinschaft und des Staates nur auf der Grundlage sorgfältiger Beobachtung der Realität und rationaler Argumentation gebildet werden soll. Rationalität ist die Basis guter Politik. Dass der dabei verwendete Qualitätsbegriff vielfältigster Interpretation zugänglich ist, ändert nichts. Trotzdem sind größte Zweifel angebracht, ob Beteiligungsphilosophie und Qualitätsstreben zu denselben Ergebnissen führen.

224 Vgl. z.B. Art. 72 der Bremer Verfassung, Art. 50 der Hamburger Verfassung, Art. 60 der Verfassung von Mecklenburg-Vorpommern.

Können wir *jedes* Produkt eines „mitbestimmten" Entscheidungsprozesses für „besser" halten, verglichen mit Entscheidungen durch Repräsentanten? Die Geschichte der westlichen Demokratien spricht eindeutig gegen diese Auffassung. Nur in extremen Situationen, nämlich in Revolutionen schafft die unvermittelte Selbstbestimmung des Volkes eine neue Ordnung, die allgemein als Fortschritt angesehen wird. Solange eine im Kern demokratische Repräsentativverfassung gilt – also bei hinreichenden Möglichkeiten für das Volk, sich in Wahlen und Abstimmungen verbindlich zu äußern –, sind Volksentscheide nicht schon deshalb „besser", weil sie eben Entscheidungen des Volkes und nicht der Parlamente oder Regierungen sind. Sie sind es nur deshalb, weil es angemessen ist, dass die Menschen sich möglichst weitgehend „selbst regieren".

Dass über das Internet heute ein großer Teil der Weltbevölkerung – wenn auch noch lange nicht die gesamte – Zugang zum Wissen der Welt haben kann, dass die Völker also ihre Geschicke aufgeklärt gestalten können, ist eine wunderbare Errungenschaft unserer Zeit. Die Hoffnung, dass unser künftiges Zusammenleben auf diesem Planeten friedlicher und gerechter sein wird als es in der Vergangenheit war, beflügelt auch manche Netz-Pioniere und die „Piraten" in den verschiedenen Parteien. Nur scheint es manchmal so, als würde die Faszination des technischen Mittels von der Erarbeitung der politischen Inhalte ablenken – und das wäre eine Fehlleitung kreativer Kräfte, die wir für anderes brauchen.

Ausdruck des Glaubens an die gesteigerte Wirkung des Expertentums sind u. a. die zahlreichen Rankings und Prioritätenlisten, mit denen manche Medienerzeugnisse allerhand Geld verdienen. Wir erfahren Tausende von Zahlen, deren Bedeutung wir nicht einschätzen können, weil wir die Vergleichswerte nicht kennen, und ein großer Teil der Alltagsstatistiken ist für die Meinungsbildung des Einzelnen schlicht irrelevant – oder aber die entscheidenden Zahlen fehlen, etwa weil statt der Werte aus der Vergangenheit Prognosen benötigt werden, diese aber nicht zuverlässig erarbeitet werden können.

Umgekehrt bilden wir unsere Meinung trotz verfügbaren Zahlenmaterials in der Regel nach anderen Kriterien, und das muss nicht einmal irrational sein. Wenn etwa darüber gestritten wird, ob alle Schüler länger als vier Jahre gemeinsam unterrichtet werden sollen – das war das zentrale Thema des Schulsystemstreits in Hamburg 2010 –, dann können wir zwar mit anderen Ländern vergleichen, die das längere gemeinsame Lernen praktizieren. Aber die Ausgangsbedingungen (z.B. die Zahl von Migrantenkindern, aber auch das soziale Klima insgesamt) sind dort andere als bei uns, und auch die Experten können nicht genau vorhersagen, welche Wirkungen die Umstellung bei uns hätte. Vergleichende Überlegungen sind zwar wichtig, aber man kann es niemandem verübeln, dass er sich angesichts der Ungewissheit der Entscheidungsgrundlagen „aus dem Bauch" für die eine oder die andere Alternative entscheidet.

An Aufklärung fehlt es allenthalben. Was die Sicherheitsbehörden tun, ist immer noch mit einem Schleier des Geheimnisses umgeben – und eben deshalb sind die Bürger übertrieben misstrauisch. Die Polizei hat zwar gelernt, mit der Öffentlichkeit zu kommunizieren; sie nutzt jetzt teilweise sogar die sozialen Netzwerke, um über ihre Tätigkeit zu informieren. Die Nachrichtendienste hingegen erhalten trotz aller Transparenzforderungen die Aura des Verborgenen aufrecht. Insgesamt herrscht nach wie vor ein beängstigend großes Maß an Unwissenheit darüber, wie der Staat organisiert ist und wie er handelt. Die „Beamten" sind Objekt von Neid und Spott, aber was sie tatsächlich tun und unter welchen Bedingungen sie ihre Arbeit verrichten, ist weiten Kreisen des Volkes unbekannt. Und dass dies so ist, beruht nicht allein auf Dummheit oder Desinteresse und auch nicht allein darauf, dass die politisch Verantwortlichen nicht genug Informationsarbeit betreiben, sondern auch auf Fehlentwicklungen bei den Multiplikatoren und Meinungsbildnern, also Mängeln unserer sonst so hervorragenden Publizistik.

Die Uninformiertheit vieler Menschen hat aber noch eine andere Wurzel: Die Hersteller all der schönen Geräte, die unseren Alltag bereichern sollen, geben sich wenig Mühe, die richtigen Einstellungen und Klicks zu erklären, geschweige denn zu sagen, was wir tun sollen, wenn die Apparate nicht so funktionieren, wie sie sollen. Die Internet-Unternehmen tauschen Angebote ohne Erklärung aus, nehmen updates vor, die sich auf die Speicherung bei den Nutzern auswirken, und die Betreiber von Webseiten verstecken die Wahlmöglichkeiten, die einen strengeren Datenschutz bewirken, unter komplizierten Anordnungen der Buttons und Texte. Die Experten scheinen die Nutzer, die nur die Oberfläche der Geräte sehen und die Routinen für die schnelle Nutzung nicht kennen, für Idioten zu halten, die es nicht verdient haben, die Segnungen der Technik zu genießen. Extra große Zahlen und Buchstaben auf Handys für Senioren ändern an dieser Tendenz nichts.

Die staatlichen Stellen bemühen sich in mancherlei Hinsicht mehr. Während die Behörden früher den Versprechungen der IT-Industrie kritiklos gefolgt sind (und dadurch eine Fülle unpassender, schematischer Lösungen in die staatliche Datenverarbeitung eingeführt wurde), sind sie heute deutlich kritischer. Sie stellen Ansprüche an Industrie und Berater, gestalten ihre Geschäftsprozesse aufgabenspezifisch und beziehen rechtliche Vorgaben (einschließlich Datenschutz) von vornherein in die Systeme ein. Es gibt inzwischen eine bewusste Politik des richtigen IT-Einsatzes, etwas großspurig eine „nationale IT-Strategie" genannt. Es gibt ein Bundesamt für die Sicherheit der Informationstechnik und viele andere Stellen, auch bei den Ländern, die sich um die Datensicherheit kümmern. Damit werden übrigens zugleich Rationalisierungseffekte erzielt – was die Bestrebungen zusätzlich interessant macht. Wer seine Daten ordentlich verwaltet, Veraltetes zügig löscht und Falsches berichtigt, kann seine Aufgaben besser erfüllen als der Alles-

Sammler, der keinen Durchblick mehr hat. (Dieser Effekt ist auch den Datenschutzbeauftragten seit langem bekannt und wird von ihnen gefördert.)

Vierter Teil: Fazit und Konsequenzen

Freiheit oder Angst, Resignation oder Aufbruch?

Die Demonstranten, die ihren Protest gegen zu weit gehende Überwachung unter das Motto „Freiheit statt Angst“ stellen, kennen offenbar nur die Angst vor dem Staat. Ein großer Teil des Volkes aber hat mindestens ebenso große oder größere Angst vor Straftaten und Bedrohungen durch die Mitmenschen. Liberale Kommentatoren mokieren sich über diesen Wunsch nach Sicherheit und behaupten, wer sich für entsprechende Befugnisse der Kriminalpolizei einsetze, wolle nur die Macht der Behörden über die Bevölkerung ausbauen. Aber trotz aller Übertreibungen, die auf diesem Gebiet vorkommen, ist es unbestreitbar, dass die meisten Menschen möglichst von Kriminalität verschont bleiben, also ihre Angelegenheiten in Ruhe und Sicherheit betreiben wollen. Bei der Bekämpfung des Rechtsextremismus rufen – unabhängig von eigener Betroffenheit – sogar radikale Linke nach intensiveren Ermittlungen von Polizei und Verfassungsschutz. Es stimmt auch nicht, was polemisch immer wieder behauptet wird, dass nämlich die Politik „hundertprozentige“ Sicherheit verspreche, was ja in der Tat nicht erreichbar ist. Jeder, der etwas von den wahren Verhältnissen weiß, ist zufrieden, wenn es gelingt, die Kriminalitätsrate um ein paar Prozentpunkte zu senken, und auch dazu bedarf es einer Polizei, die mit hinreichenden Befugnissen ausgestattet ist.

Das richtige Motto der Sicherheitspolitik, die gleichzeitig den Staat in Grenzen halten will, wäre also: „Mehr Sicherheit – weniger Angst“, genauer: Mehr Sicherheit und weniger Angst vor der Verletzung von Individualrechten – sei es durch den Staat, sei es durch Private. Ein unaufgeregter, aufgeklärter Gebrauch der informationstechnischen Instrumente und die sorgfältige Beachtung der rechtsstaatlichen Grenzen staatlicher Einmischung in die private Sphäre – das muss das Ziel sein.

Der Weg dahin ist nicht einfach. Es gibt nicht die eine einzig richtige Route, sondern eine Mehrzahl von Pfaden, die parallel zueinander begangen werden können. Gesellschaftliche Selbstorganisation und staatliche Politik müssen sich ergänzen.

Macht der Computer und Gegenmacht der Nutzer

Geisteswissenschaftler, die sich wegen der Netzentwicklung Sorgen machen, übersehen bisweilen die triviale Tatsache, dass nicht „die Computer" und nicht „das Netz" Gefahren verursachen, sondern bestimmte Unternehmen als Betreiber und wir selbst als Nutzer. Die Macht liegt bei denen, die über Computer und Netz verfügen, die uns die Nutzungsbedingungen diktieren und die Entgelte bestimmen. (Dass so vieles im Internet „frei", ohne Entgelt erhältlich ist, täuscht uns über die Kosten hinweg, die an anderer Stelle entstehen und die wir auf anderem Wege ausgleichen, insbesondere durch die Überlassung von Daten zu Werbezwecken). Die schöne Freiheit der Internetnutzung bildet nur die Fassade ganz gewöhnlicher wirtschaftlicher Austauschverhältnisse, die im Hintergrund stattfinden. Die großen Internetanbieter nutzen ihre wirtschaftliche Macht, um Konkurrenten kleiner zu machen und die Nutzer zu noch intensiverer Nutzung zu veranlassen. Die Informationsmassen, die in den Servern gespeichert sind, können auch anderen Interessen dienstbar gemacht werden; sie stärken unter Umständen die Macht von Unternehmen oder Behörden. Aber auch in diesem Zusammenhang kommt es darauf an, ob jemand sich tatsächlich dieser Informationen bedient; die Apparate und Leitungen selbst sind weder aktive noch potentielle „Machthaber".

Damit ist aber zugleich gesagt, dass auch Gegenmacht vorhanden ist. Jede demokratische Regierung hat eine Opposition, fast jedes Unternehmen hat Konkurrenten, und die Bürger wie die Kunden können sich gegen die Macht der Datenverarbeiter wehren.[225] Gegen Schnüffelei und Datenmissbrauch kann jeder die Datenschutzbeauftragten oder ein Gericht anrufen; gegen unmäßige gezielte Werbung hilft besonders das Verbraucherschutzrecht. Gegen zu große Marktmacht können die Kartellbehörden vorgehen – das ist freilich ein äußerst mühsames Geschäft, vor allem international. Aus Angst vor dem Internet oder aus Ärger über unfaire Methoden der Anbieter entsteht öffentlicher Protest; aus Angst der Anbieter vor der Konkurrenz erwachsen rechtliche und politische Auseinandersetzungen über die Regeln des Wettbewerbsrechts und ob sie eingehalten worden sind oder nicht. Man braucht nicht immer erst neue Gesetze oder scharfe behördliche Maßnahmen, um Fehlentwicklungen aufzuhalten – im Gegenteil: viel wirksamer ist oft die öffentliche Demonstration von Unbehagen und Widerwillen. Die Reaktion des Gesetzgebers und der Exekutive folgt regelmäßig nach, und manchmal werden geltende Gesetze überhaupt erst wahrgenommen, wenn sie in skandalöser Weise missachtet worden sind.

225 Mit Recht wird aber gefordert, „wirksamere Möglichkeiten selbstorganisierter Kontrolle durch Nutzer" mittels „normativer Absicherungen, etwa von mehr Transparenz" zu unterstützen (Hoffmann-Riem 2012, Ms. S. 27).

Der wortgewaltige Protest von Netznutzern gegen die Pläne zur Sperrung kinderpornographischer Internetseiten war ebenso wirkungsvoll wie die Auflehnung gegen Google Street View. Die um die Kinder besorgte Familienministerin Ursula von der Leyen wurde als „Zensursula" veralbert, und die Weltfirma Google sah sich durch öffentliche Aufregung (und den besonders energischen Einsatz des Hamburger Datenschutzbeauftragten) genötigt, Hausbesitzern und Mietern ein Widerspruchsrecht gegen die Abbildung ihrer Außenwände im Internet einzuräumen. Die deutschen Verleger und ihre Rechtsvertreter konnten verhindern, dass Google in den USA für einen Spottpreis die Reproduktionsrechte für Millionen alter Bücher erhielt. Was bisher nicht ausreicht, ist zum Beispiel eine wirksame Kontrolle der Allgemeinen Geschäftsbedingungen, mit denen Google & Co. sich eine ihnen passende eigene Rechtsordnung gegeben haben. Auch wenn diese AGB unter dem Druck der öffentlichen Kritik gelegentlich ein wenig geändert werden – eine sichere Basis für das Einverständnis der Nutzer mit den Praktiken der Internet-Riesen können sie schon deshalb nicht bilden, weil sie den meisten Nutzern unverständlich sind.

Viele Internetnutzer setzen auf die netzkonforme Organisation von Widerstand, wenn ihnen die Praktiken der Anbieter unfair erscheinen. Sie gehen dabei mitunter in der Wahl der Mittel bis an die Grenzen des Erträglichen, manchmal mit Hackerangriffen auch darüber hinaus. Eine nicht-staatliche Verhaltensordnung für das Internet existierte aber in Gestalt der „Nettiquette",[226] die von Nutzern selbst entwickelt worden ist, schon vor längerer Zeit. Selbstregulierung findet nicht nur zwischen den Dienstleistungsunternehmen statt (mit der Gefahr, dass daraus rechtswidrige Kartellabsprachen werden!), sondern auch unter den Nutzern.

Hacker als Agenten des Fortschritts?

Wir mögen einfache Erklärungen für komplizierte Sachverhalte. Die Risiken der Computertechnik sind schwer erklärbar, deshalb behelfen sich manche Kommentatoren mit einer pauschalen Schuldzuweisung, möglichst an „den Staat". So lesen wir in einer Zeitung, der unsorgfältige Umgang mit Daten – die „Datenschluderei" – habe „System", und dieses System ziehe sich „durch die gesamte westliche Welt, weil kein Staat die verantwortungslosen Datenmanager in Unternehmen und Behörden zur Rechenschaft zieht". Man lasse sie gewähren, „wie man früher Walfänger und Ölkonzerne gewähren ließ". „Anders ausgedrückt: Der Staat versagt."[227] Der Autor lobt das „Hacker-Netzwerk Anonymous" dafür, dass es einen großen Datendiebstahl begangen hat. Das sei zwar ein Verstoß gegen geltendes

226 S. dazu Plotkin 2011, S. 136 ff.
227 Hamann 2011.

Recht gewesen, aber weil die bestohlene Firma Kundendaten unverschlüsselt verwaltet habe und man infolge einer Schwachstelle im Computer der Firma auf diese Daten zugreifen konnte, hätten die Hacker ebenso „ehrenwert" gehandelt wie die Greenpeace-Aktivisten, die gegen Walfang und Meeresverschmutzung gekämpft haben. Nicht die Profitgier habe die Hacker von Anonymous getrieben, sondern „die gute Sache oder das, was sie dafür halten".

Soll denn aber jeder, der eine Sache gut findet, sie ohne Rücksicht auf geltendes Recht durchsetzen? Sind die Hacker, die andere auf den Weg der datentechnischen Tugend führen wollen, die modernen Robin Hoods, die Verteidiger der individuellen Freiheit, die Agenten des Fortschritts? Handeln Datendiebe, die auf Schwachstellen aufmerksam machen wollen, sozusagen in Ersatzvornahme für den Staat? Die Fragen stellen heißt sie verneinen – wenn alle so handelten, wäre gar kein Staat mehr zu machen, sondern es würde Unordnung herrschen. Man braucht gar nicht einmal zu prüfen, ob der behauptete gute Zwecks des Hackens nicht vielleicht der Werbung für Sicherheitsdienstleistungen dienen sollte – jedenfalls ist die Heroisierung des Regelverstoßes kein brauchbares Rezept, um die weltweite „Datenschluderei" zu verhindern.

Der Chaos Computer Club, der vor dreißig Jahren gegründet wurde, um Hackern eine Plattform zu geben und über Aktivitäten berichten zu können[228], nach seiner Selbsteinschätzung[229] „die größte europäische Hackervereinigung und seit 25 Jahren Vermittler im Spannungsfeld technischer und sozialer Entwicklungen" – dieser Club gilt gegenwärtig allgemein als seriöser Verein von Experten, die sich um die Sicherheit des Netzes verdient gemacht haben; seine Sprecher wie Frank Rieger und Constanze Kurz schreiben kultur- und politikkritische Artikel in der Frankfurter Allgemeinen Zeitung und dienen Bundestags- und Landtagsausschüssen in Anhörungen als Sachverständige für Fragen der Informatik und ihrer sozialen Risiken. Auch der CCC hat sich durch mancherlei Hacker-Erfolge profiliert – und war manchmal auf der falschen Spur. Insgesamt aber scheinen die „Chaos"-Hacker überlegt und vorsichtig vorgegangen zu sein.

Die Hacker-Ethik, die der CCC propagiert,[230] ist recht allgemein formuliert. Vom Eindringen in fremde Datenverarbeitung ist da gar nicht die Rede; das wird offenbar als die „normale" Aktivität eines Hackers vorausgesetzt, und die Frage nach der Rechtmäßigkeit wird in diesem Papier nicht thematisiert. Die ersten Sätze dieser Hacker-Ethik lauten: „Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein. Alle Informationen müssen frei sein". Als spätere Hinzufügung steht am Schluss aber: „Mülle nicht in den Daten anderer Leute" und „Öffentliche Daten nützen,

228 Zur chaotischen Geschichte des CCC vgl. den einschlägigen Wikipedia-Artikel.
229 Natürlich im Internet: www. chaoscomputerclub.de .
230 Im Internet unter www.ccc.de/hackerethik.

private Daten schützen“. Dass hierin ein Widerspruch liegt – die „Daten anderer Leute“ und die „privaten“ Daten sind dann eben doch nicht frei –, wird nicht zum Ausdruck gebracht. Doch wird durch die Änderungen deutlich gemacht, dass man nicht mehr ohne Rücksicht auf die Folgen hacken will. Wörtlich heißt es: „Auch Eingriffe in die Systeme fremder Betreiber wurden zunehmend als kontraproduktiv erkannt“. Geradezu weise lautet es am Schluss: „Die Hackerethik befindet sich – genauso wie die übrige Welt – insofern in ständiger Weiterentwicklung und Diskussion“.

Als Befreier von allen „Datenschludereien“ dürften die Hacker also auch nach eigener Einschätzung nicht berufen sein. Aber vielleicht tragen sie wirklich zu einer neuen Computer-Ethik bei, die nicht nur in der Leugnung traditioneller Rechtsprinzipien besteht.

Verantwortung für Datensicherheit

Damit die rechtlichen Grenzen der Datensammlung und -verwendung tatsächlich eingehalten werden, bedarf es der Daten*sicherung* (die insofern vom Datenschutz abzugrenzen ist). Sicherheit zu gewährleisten – im Netz und in den angeschlossenen Computern – ist eine riesige Aufgabe für die Verantwortlichen, aber primär verantwortlich für die Einzelheiten und für die Durchführung ist nicht der Gesetzgeber, sondern es sind die Betreiber und Nutzer der Datenverarbeitung – Unternehmen, Behörden und Private. Der Gesetzgeber kann insofern auf den Stand von Wissenschaft und Technik verweisen, so wie er es auch beim Umweltschutz, bei der Reaktorsicherheit und in vielen anderen Bereichen tut.

Zwar hat das Bundesverfassungsgericht (im Urteil über die Vorratsdatenspeicherung) dem Gesetzgeber aufgegeben, auch die Sicherung der Daten penibel zu regeln. Es ist damit aber weiter in die Details gegangen, als nötig wäre, und hat einem Misstrauen gegen alle Anwender Ausdruck verliehen, das eher kontraproduktiv als hilfreich wirken wird. Denn diejenigen, die den Datenverarbeitern nur Schlechtes zutrauen, werden sich gerade durch solche Urteile bestätigt fühlen, und die anderen werden zu grübeln beginnen, ob die Angst vor Missbrauch nicht doch etwa begründet sei, wenn schon die höchsten Richter sie ernst nehmen.

Die praktischen Schwierigkeiten bei der Sicherung sensibler Daten beruhen nicht darauf, dass die Normen ungenau und mehrdeutig sind. Viel bedrohlicher ist die „Cyber-Kriminalität“ in ihren zahlreichen Varianten. Sie ist längst international

organisiert und deshalb mit nationalstaatlichen Instrumenten schwer zu fassen.[231] Von Regierung und Parlament dürfen wir erwarten, dass sie auf diesem Gebiet besonders aktiv sind. Nur aufgrund europarechtlicher Normen und internationaler Abkommen und durch supra- und internationale Behörden kann die Internet- und Computerkriminalität wirksam bekämpft werden.

Regulierte Selbstregulierung als pragmatisches Konzept

Bei allem Eifer der Gesetzgeber auf nationaler und supranationaler Ebene: Die Internet-Unternehmen sind in der Verantwortung, die Strukturen und Prozesse der Informationsverarbeitung zunächst einmal selbst zu ordnen – und zwar gerecht zu ordnen. Sie sind als marktbeherrschende Unternehmen oder Oligopolisten verpflichtet, eine Ordnung zu schaffen, die den Interessen der verschiedenen Gruppen von Kunden entgegenkommt; eigene Interessen dürfen nicht unbeschränkt verfolgt werden. Nebenbei gesagt, ist das schon um der Zufriedenheit der Kunden willen geboten. Dass sie diesem Anspruch tatsächlich gerecht werden, bezweifeln viele.

In der Netzgemeinde wird Selbstregulierung vielfach misstrauisch betrachtet, vielleicht weil – wie Karl-Heinz Ladeur meint – „der quasi-anarchische Charakter des Internet als förderlich für die Freiheit der Kommunikation angesehen wird".[232] Ladeur plädiert demgegenüber dafür, die „social media" wie Facebook als „Netzwerk von Verträgen" anzusehen, das die Regeln ständig weiterentwickelt und das „zu einer eigenständigen, ‚netzgerechten' Weiterentwicklung des Privatrechts und zur Institutionalisierung neuer Formen für die Rechtsbeziehungen im Internet" beiträgt.[233] Konflikte um den Datenschutz in den sozialen Medien könnten nach seiner Ansicht in einem Online-Mediationsverfahren vor einem (von Unternehmensorganen unabhängigen) „Cyber-Court" verhandelt werden.

Die „Selbstregulierung" ersetzt nicht die Rechtsetzung durch den Staat und die supranationalen Instanzen, sie ist nach allen Erfahrungen überhaupt nur „im Schatten des Rechts", vor dem Hintergrund möglicher staatlicher Regelung wirksam. So verstanden, kann sie die Gesetzgeber entlasten, und sie kann in vielen Punkten angemessener ausfallen als die von außen auferlegten Normen.[234] Sie muss Gleichbehandlung garantieren und bei Verstößen Sanktionen vorsehen, die auch durch-

231 Zu den entsprechenden Ansichten und Einschätzungen des Bundeskriminalamts vgl. den Bericht, den das Deutsche Institut für Vertrauen und Sicherheit im Internet über eine Expertenrunde der Enquete-Kommission „Internet und digitale Gesellschaft" am 28. 11. 2011 in Berlin verfasst hat (www.divsi.de/node/55). S. a. oben S. 78 f.

232 Ladeur 2012, S. 5.

233 Ebd. (auch die folgende Aussage).

234 So auch der Tenor der Diskussion auf der Datenschutz-Konferenz des Bundesministeriums des Innern und des Alexander von Humboldt-Instituts für Internet und Gesellschaft am 17./18.10.2012 in Berlin, Panel 3 (unveröff. Bericht von Thomas Kranig und Martin Eifert).

geführt werden. Dieses Instrument der „regulierten Selbstregulierung“ ist auch auf anderen Gebieten inzwischen als brauchbar und bürgerfreundlich anerkannt. Es ist jedenfalls für einige wichtige Streitfälle im Internet wahrscheinlich sogar besser geeignet, z.B. für die Festlegung fairer Regeln für Bewertungs- und Rating-Systeme oder Diskussionsforen.[235]

Subsidiär aber bleibt immer der Staat in der Pflicht, die Grundrechte der Bürger zu schützen. Daraus folgt, dass er Pflichten der Betreiber festlegen kann, ihrerseits an dem Schutz der Grundrechte mitzuwirken. Die Diensteanbieter dürfen vor offensichtlichen Persönlichkeitsverletzungen nicht die Augen verschließen, sie können sogar mit einer – wenn auch begrenzten – Beobachtungspflicht belegt werden.[236] Das leuchtet zwar manchen Internet-Freunden nicht ein, aber es ist die zwingende Konsequenz daraus, dass manche Interessenkonflikte nur im Zusammenwirken der Betreiber und der Aufsichtsbehörden bewältigt werden können.

Die Pläne von Parteien und Regierungen

Sage niemand, die politischen Parteien beschäftigten sich nicht mit „Netzpolitik“. Sie haben Arbeitskreise gegründet, Berichte entgegengenommen und Parteitagsbeschlüsse gefasst. Die diskutierten und beschlossenen Papiere enthalten viel politische Lyrik, populär-philosophische Aussagen und praktische Appelle, daneben die übliche Kritik an der Konkurrenz. Man muss schon gründlich lesen, um herauszufinden, welche Linie die Parteien empfehlen.

Es sind zunächst nur Nuancen, in denen sich die verschiedenen Meinungsgruppen voneinander unterscheiden. Selbstverständlich bekennen sich alle relevanten Kräfte dazu, dass das Bekenntnis zur Menschenwürde als der obersten Norm des Grundgesetzes allen anderen Geboten vorangeht. Und alle wollen, dass die „Grundwerte“ den Kurs bestimmen; bei den beiden großen Parteien liest sich das so: „Freiheit, Solidarität und Gerechtigkeit“ (CDU)[237] oder „Freiheit, Gerechtigkeit und Solidarität in der digitalen Gesellschaft“ (so hat die SPD ihren Parteitagsbeschluss überschrieben)[238]. Differenzen ergeben sich aber sogleich bei der Akzentuierung und erst recht bei der Durchführung dieser Großziele. Das muss auch so sein und entspricht der Aufsplitterung des ganzen Volkes in große Meinungsblöcke. Die einen betonen die Freiheit (des Individuums) und – in einem Spannungsverhältnis dazu – die Sicherheit (der Menschen und ihrer Rechtsgüter), während

235 Vgl. die Hinweise von Ladeur 2009, S. 34 ff.
236 Ladeur 2009, S. 41 ff. zum Jugendschutz.
237 24. Parteitag der CDU Deutschlands, Bericht des Arbeitskreis (sic) Netzpolitik, S. 2, im Internet unter www.netzpolitik-cdu.de. Die CSU hat einen „Netzrat“ eingerichtet, der am 31.1.2011 ein umfangreiches Positionspapier veröffentlicht hat.
238 Bundesparteitag der SPD, 4.-6.12.2011 (einstimmig beschlossen).

die anderen die soziale Gerechtigkeit und die demokratische Ordnung des Gemeinwesens herausstellen. Die eine Seite sagt: „So viel Staat wie nötig, so wenig wie möglich“, die andere fragt nach den gesellschaftlichen Problemen und fordert den Staat auf, sie zu beheben. In vielen Details sind die Gruppen sich sehr nahe, in anderen stehen sie sich sehr fern.

Dem üblichen parteipolitischen Stil entsprechend, wird zunächst überall die *Freiheit* in ihren verschiedenen Formen beschworen: Freiheit des Individuums zur Persönlichkeitsentfaltung, Freiheit des Internets vor Zensur und anderen staatlichen Eingriffen, Freiheit von Viren und Trojanern. Zwar fordern die etablierten Parteien nicht die allgemeine Freiheit von rechtlichen Bindungen, wohl aber die Unbefangenheit der Kommunikation über das Netz – und damit taucht unausgesprochen schon der grundlegende Zielkonflikt auf. Am unbefangensten kann ich kommunizieren, wenn kein Dritter meine Äußerungen zur Kenntnis nimmt und niemand mich dafür verantwortlich machen kann. Aber wenn das Internet ein „rechtsfreier Raum“ wäre, könnten sich einige rücksichtslose Nutzer darin zu Lasten aller anderen „austoben“. Der größere Teil der Nutzer würde sich dann bald ganz vom Netz abwenden oder nur noch einen kleinen Ausschnitt der Angebote nutzen. Das heißt: Mit den allgemeinen Beschwörungen der individuellen Freiheit ist es nicht getan, umstritten sind immer die Einzelfragen. Da aber hapert es vielfach an klaren Aussagen.

Alle sind für den Ausbau der Infrastruktur, für hochleistungsfähige Breitbandkabel oder für ein kabelloses Funknetz für das Internet. Alle betonen, dass jeder die Chance haben muss, über das weltweite Netz mit jedem anderen zu kommunizieren. Dabei sind die Sozialdemokraten dafür, die Grundversorgung aller Einwohner dadurch zu gewährleisten, dass marktbeherrschenden Unternehmen eine „Universaldienstpflicht“ auferlegt wird[239], während die Christdemokraten mehr auf den Wettbewerb setzen, der auch in dünnbesiedelten Gegenden für Empfangs- und Sendemöglichkeiten sorgen werde[240]. Auch die Vertreter der reinen Marktwirtschaft dürften bereit sein, den Staat für die Ausfüllung von Versorgungslücken in die Pflicht zu nehmen. Die SPD fordert sogar, dass der Staat die IT-Unternehmen im „Kampf gegen Viren und Spams“ unterstützt.[241]

Die SPD versteht sich als „Partei der digitalen Demokratie“. Diese leicht pathetische und sprachlich falsche[242] Formel wird zum Glück nicht weiter inhaltlich aufgeladen, sondern sogleich relativiert: „Digitale Demokratie ist weder Selbstzweck noch ein von der sogenannten ‚realen Welt‘ abzutrennender Bereich der demokratischen Politik. Sie macht weder demokratische Entscheidungen in den

239 SPD-Bundesparteitag (vorige Fn.), Zeile 124 ff.
240 Bericht des CDU-Arbeitskreises Netzpolitik zum Parteitag 13.-15.11.2011, S. 10.
241 SPD-Parteitagsbeschluss (Fn. 238), Z. 138 ff.
242 S. oben II. Kapitel.

Parteien überflüssig noch kann sie sie ersetzen. Aber sie erleichtert demokratische Verfahren und Partizipationsmöglichkeiten in einem erheblichen Ausmaß.“ Diese Chance will die SPD nutzen.[243]

Natürlich beschäftigen sich auch die anderen Parteien mit Netzpolitik. Die „Grünen“ bekunden auf ihrer Internetseite ihre Solidarität mit den Protesten gegen die amerikanischen Gesetzesvorhaben PIPA und SOPA und verkünden „Offenheit, Freiheit, Teilhabe“. Selbstverständlich finden sich auch die flotten Sprüche wie „Deine Daten gehören dir“ und „Datenschutz ist Bürgerrecht“. „Die Linke“ nimmt die üblichen Stichworte ebenfalls auf, tut sich aber schwer mit dem Urheberrecht; sie will es „aktualisieren“.

Und was wollen die Piraten, die nach ihrem Einzug in das Berliner Abgeordnetenhaus als ernstzunehmende politische Partei, als jugendfrische Neuauflage der inzwischen etablierten Grünen gelten? Sie wollten die „Generation Netz“ in die Politik einbringen – einschließlich ihrer ungenierten Neigung zum Kopieren und Downloaden über die Grenzen des bisher Erlaubten hinaus. Damit gehört die Änderung des Urheberrechts auf die Agenda der Piraten,[244] und vielleicht kann man von ihnen außer dem Protest gegen ACTA tatsächlich noch Kreatives zu diesem Thema hören. Zunächst aber haben sie andere Forderungen auf ihre Fahnen geschrieben.

Wie eine Satire mutet bei all dem der Aufruf eines CDU-Bundestagsabgeordneten an, der offenbar ernsthaft meint, die „digitale Revolution“ gefährde die bürgerlichen „Werte von Freiheit, Demokratie und Eigentum“. Das Web 2.0 werde bald Geschichte sein; bis dahin werde noch viel „digitales Blut“ vergossen werden. Die „digitale Avantgarde“ rückt er in die Nähe von „Maoisten“. Ansgar Heveling, der Autor solcher apokalyptischen Albträume,[245] ist immerhin Mitglied der Enquete-Kommission „Internet und digitale Gesellschaft“. Er spricht aber offensichtlich nicht für die CDU; Parteifreunde haben sich sogleich von seiner Attacke distanziert, darunter die Vorsitzende des CSU-Netzrates, Dorothee Bär. Seine „sinnlose Polarisierung“ lenkt nur von der Problemlösung ab und wird bald vergessen sein.[246]

Die Bundesregierung hat schon vor einiger Zeit die Skizze eines „Rote-Linie-Gesetzes“ veröffentlicht.[247] Sie ist als Teil einer übergreifenden Netzpolitik gedacht, zu der u.a. auch gehört, dass „die Chancen der Digitalisierung des öffentlichen Raumes“ genutzt werden. Experten auf Bundes- und Länderebene bemühen sich intensiv um die effektive und effiziente Nutzung der Informations- und Kom-

243 SPD-Parteitagsbeschluss (Fn. 238), Z. 175 ff.
244 Vgl. dazu von Gehlen 2011 (unter Berufung auf den schwedischen Piraten-Gründer Rick Falkvinge).
245 Heveling 2012; dazu u.v.a. Graff.2012 (dort auch die Zitate).
246 Graff 2012.
247 Mehr dazu unten S. 139 ff.

munikationstechnik für die öffentliche Verwaltung. Der von beiden Ebenen beschickte IT-Planungsrat hat eine „Nationale E-Government-Strategie" formuliert,[248] und die Bundesregierung hat ein Regierungsprogramm „Vernetzte und transparente Verwaltung" beschlossen.[249] Damit sind u.a. Projekte wie die einheitliche Behördenrufnummer 115 und der sichere elektronische De-Brief gemeint. Ein Baustein in diesem Modernisierungsprozess soll auch das Vorhaben „Open Government" (Offenes Regierungs- und Verwaltungshandeln) sein.

Das Nachdenken darüber führt über die pragmatische Problemlösung hinaus bis ins Visionäre: In einer Studie „Vom Open Government zur Digitalen Agora" liefert ein einschlägiger Think-Tank für das Bundesinnenministerium einen interdisziplinären Diskussionsbeitrag voller hochfliegender Ideen.[250] Der kühne Vergleich ist ernst gemeint: Die Autoren erhoffen sich von der elektronisch gestützten Kooperation, Transparenz und Partizipation eine Renaissance der Agora, also des Forums, auf dem im antiken Athen und Rom Politik betrieben und Geschäfte abgeschlossen wurden. Die Verknüpfung der Akteure in einem „Netzwerk gleichberechtigter Partner" werde auch ein „Innovationstreiber für die Wirtschaft" sein. „Im Kern" handle es sich „um nichts Geringeres als die zeitgemäße Ausführung der Markt- und Versammlungsplätze in den Städten des antiken Griechenlands, die gleichzeitig Ort von Politik, Handel und sozialer Interaktion waren: eine Digitale Agora".[251] Ein schönes Bild – aber an anderer Stelle dieses Papiers heißt es mit Recht: „Schon einiges erreicht – und noch viel zu tun".[252] Die Entwicklung muss „von den Werkzeugen abstrahiert und als politisches und institutionelles Phänomen verstanden"[253] werden. Da ist es wohl nur ein Ausrutscher, wenn es am Ende (der Zusammenfassung) heißt, die heutige IT-gestützte Verwaltung sei „die Basis für die aktuelle Entwicklung".[254] Politisches Handeln sollte nicht beim Stand von Technik und Organisation, sondern bei den sozialen, administrativen und wirtschaftlichen Problemen ansetzen und zunächst die neuen Bedarfe feststellen, bevor die Prozesse umgestellt werden.

248 Beschluss vom 24.10.2010 (www.it-planungsrat.de).
249 Bundesministerium des Innern (Hrsg.), Regierungsprogramm „Vernetzte und transparente Verwaltung", Sept. 2010 (www.verwaltung-innovativ.de).
250 Kammer/ Huppertz/Westerfeld 2011.
251 Ebd., S. 3 f.
252 Ebd. , S. 5.
253 Ebd. , S. 1
254 Ebd. , S. 6.

Was also heißt Netzpolitik?

„Netzpolitik" ist gegenwärtig ein Konglomerat von Wünschen und Forderungen, die nur lose miteinander verknüpft sind. Das Ziel, eine „bessere Welt" zu schaffen, ist allen gemeinsam, die sich für die Ordnung von Staat und Gesellschaft engagieren, aber es taugt nicht als Abgrenzungsmerkmal zu anderen Politikfeldern. Es gibt kein allgemein gültiges Konzept zur Lösung aller Probleme der neuen Techniken.

Eine weltweite technische Revolution und ihre ökonomischen, sozialen und politischen Folgen lassen sich nicht in einfachen, allgemein gültigen Rechtsnormen einfangen und einhegen. Deshalb empfiehlt es sich, die unterschiedlichen Fragenkreise auseinanderzuhalten und je für sich zu diskutieren. Nur auf diesem Wege fließen die materiellen Gehalte in die Überlegungen ein, die im geltenden Recht vorhanden sind und an die man anknüpfen kann. Die Lösungen müssen den technischen und sozialen Sachverhalten gerecht werden, sie müssen zukunftstauglich sein, aber sie entstehen nicht aus den Eigenschaften der Technik, sondern aus der Beobachtung der jeweils beteiligten und betroffenen Interessen und der sozialen Praxis und insbesondere der Klärung dessen, was wir wollen. Einfacher gesagt: Aus dem „Sein" der Technik und ihrer Anwendungsformen folgt nicht ohne weiteres das „Sollen"; die Normen müssen oft gerade gegen die Fakten gewonnen und durchgesetzt werden.

Diese Anforderung an den Normsetzungsprozess führt dazu, dass diejenigen, die für die *Anwendung* der Technik zuständig sind, auch den Sachverstand und die Werteskala einbringen müssen, die das künftige Spezialrecht prägen. So sind zur Gestaltung des Arbeitnehmerdatenschutzes nicht nur Experten für Datenverarbeitung heranzuziehen, sondern die Arbeitsrechtler, die sich regelmäßig mit ähnlichen Fragen befassen. Das Gesetz über den Datenschutz für Arbeitnehmer sollte von dem Ministerium erarbeitet werden, das sich sonst mit Arbeitsrecht befasst, eben dem Arbeitsministerium. Das für die allgemeinen Fragen des Datenschutzes zuständige Ressort – das Innenministerium – kann und soll seinen Sachverstand mit einbringen, aber nicht federführend sein. (Das heißt natürlich nicht, dass die Experten ihre Vorstellungen voll durchsetzen sollen, sich sozusagen „ihr eigenes Gesetz machen"; das Parlament korrigiert einseitig fachspezifische Gesetzentwürfe aufgrund seiner allgemein-politischen Verantwortung und Erfahrung!).

Was also sollte Netzpolitik bedeuten, wie sollte sie vorgehen?

Zu allererst: Nicht jedes neue Thema muss sogleich vom Gesetzgeber aufgegriffen werden. Die nötigen Regeln entstehen auch ohne gesetzgeberische Aktivität: durch Anwendung bestehender Normen und Prinzipien, durch vernünftige Praxis der Anwender, durch richterliche Rechtsfortbildung. Eine Fülle von Rechtsnormen wird ständig von den Gerichten produziert und von Rechtsanwälten und

Professoren kommentiert und rechtspolitisch weiterentwickelt.[255] Gute Gesetzgebung setzt Erfahrung mit einer Vielzahl gelöster Fälle voraus, und sie braucht Zeit.

Die Verantwortung des Staates für Persönlichkeits- und Datenschutz

Der Persönlichkeitsschutz hat in Deutschland und in vielen anderen Staaten eine lange Tradition und ist auch im internationalen Recht befestigt. Weil sich dieses Recht weitgehend bewährt hat, brauchen wir keine umfassende Neukonzeption, wohl aber durchdachte Verbesserungen und ein konkretes Eingehen der Gesetzgebung auf die ökonomische und technische Entwicklung – aber gerade nicht Anpassung an die jeweils neueste Technik.

Das Dauerthema Sicherheitspolitik

Besonders häufig wird darüber gestritten, wie weit der Staat bei der Aufklärung und Verfolgung von Straftaten und der Abwehr von Gefahren für die Allgemeinheit in die Privatsphäre der Bürger eindringen darf. Die Sicherheitsgesetze und die Sicherheitsbehörden standen und stehen im Zentrum des öffentlichen Interesses und der öffentlichen Kritik. Diese Diskussion ist vorübergehend abgeebbt, aber sie wird wieder aufleben, sobald wieder besonders schwere Straftaten geschehen oder die Sicherheit bedroht erscheint. Sie ist notwendig und hat in der Vergangenheit zu vernünftigen, rechtsstaatsfreundlichen Eingrenzungen geführt, auch wenn nicht alle kritischen Punkte ausgeräumt sind.[256]

Die sicherheitspolitische Diskussion sollte aber von den übrigen Auseinandersetzungen um den Datenschutz getrennt werden; es gibt nur wenige Schnittstellen, und die allgemeinen rechtlichen und politischen Fragen um die Entwicklung des Datenschutzes (die ich im Folgenden noch einmal zusammenfasse) haben deutlich geringeres Gewicht als die Probleme von Polizei, Justiz und Nachrichtendiensten.

255 Als Beispiele für diesen Zweig der Rechtsentwicklung: Härting 2005; Haug 2010; Heckmann 2011; Wien 2012. Zum Internetrecht, wie diese und zahlreiche andere Autoren es behandeln, zählen vorrangig die zivilrechtlichen Fragen um die richtige Vertragsgestaltung und -auslegung, differenziert nach den verschiedenen Arten von Dienstleistern, aber auch das Recht der Domains, der Internetauktionen und der Wettbewerbsbeziehungen, das Fernabsatzrecht u.v.a.

256 Dazu Bull 2011 a, S. 67 ff., 85 ff.

Datenschutz ist kein Allheilmittel und kein Selbstzweck

Der Persönlichkeitsschutz durch Datenschutz ist eine große Errungenschaft der Rechtskultur, aber kein Patentrezept und Allheilmittel, um der Entwicklung des Internets Herr zu werden – und zwar nicht etwa deshalb, weil das Datenschutzrecht veraltet wäre – für große Bereiche der Datenverarbeitung enthält es nach wie vor die wesentlichen Richtlinien und viele Einzelregelungen, die den Umgang mit persönlichen Daten in der Praxis beeinflusst haben. Die Gesetze und vor allem die Tätigkeit der Datenschutzbeauftragten haben allenthalben das Bewusstsein dafür geschaffen, dass man mit den Informationen über andere Menschen sorgsam umgehen muss. Auch diejenigen Anwendungen der Informations- und Kommunikationstechnik, die in den letzten Jahren neu entwickelt wurden, sind – jedenfalls zum Teil – bereits in neuen Gesetzesnormen berücksichtigt; so ist das Telekommunikationsrecht höchst differenziert ausgebaut worden, und die Datenschutzregeln für die Sicherheitsbehörden sind – entgegen dem Anschein, der durch besonders kritische Berichterstattung erweckt wird – immer wieder Gegenstand von Nachbesserung und Weiterentwicklung. In der aktuellen Auseinandersetzung mit der EU-Kommission über ein künftiges einheitliches Datenschutzrecht wird plötzlich auch vielen Skeptikern klar, dass in Deutschland gerade die Sicherheitsbehörden relativ streng reguliert sind.

Aber unser Datenschutzrecht leidet unter überzogenen Erwartungen und großen Missverständnissen. Statt vom Schutz der Individualrechte beim Umgang mit personenbezogenen Daten, wie er in den letzten Jahrzehnten entstanden ist, wird verkürzt und einseitig vom Recht auf „informationelle Selbstbestimmung“ gesprochen.[257] Die neue Formel klingt überaus bürgerfreundlich, und sie verspricht die Durchsetzung einer neuen, umfassenden Freiheit des Individuums. Es ist natürlich auch angemessener, dass der Staat die Selbstbestimmung des Einzelnen schützt, statt „die Daten“ zum Gegenstand von Rechtsvorschriften zu machen. Doch der Schutz der Daten ist schon immer als Schutz menschlicher Interessen verstanden worden; nur so macht er Sinn. Datenschutz darf nicht zum Selbstzweck werden.

Der entscheidende Einwand gegen die Rechtsfigur der „informationellen Selbstbestimmung“ ist jedoch: Es genügt nicht, nur das eine Interesse, also die Selbstbestimmung der Betroffenen zu verteidigen, sondern die Gesetze müssen gerade auch Interessen*konflikte* in den Blick nehmen. Als Mitglied der menschlichen Gemeinschaft bin ich nicht in der Lage – und soll es auch nicht sein – auszuschließen, dass andere etwas über mich erfahren. Meine Geheimnisse müssen geschützt werden, aber nicht alles ist Geheimnis, was ich im Rahmen von privaten Beziehungen,

257 Kritik an dieser Rechtsfigur: Bull 2011 a, S. 29 ff., 40 ff. Dort findet sich auch eine eingehende Auseinandersetzung mit der einschlägigen Literatur und Rechtsprechung. Kritisch u.a. auch Ladeur 2009, S. 31 ff.

geschäftlichen Verhandlungen und beruflichen Kontakten über mich preisgebe. Meine Partner wollen mit Recht manches über mich wissen, zum Beispiel wenn sie mir etwas liefern sollen, mich als Arbeitnehmer beschäftigen oder ein gemeinsames Projekt betreiben wollen – und in vielen anderen Konstellationen, in denen ich mich mit anderen zusammen- oder auseinandersetze.

Die „informationelle Selbstbestimmung" ist daher als Tatbestandselement eines Grundrechts ungeeignet. Der zu schützende Rechtskreis des Betroffenen, der „Schutzbereich" des Grundrechts, wird damit nicht klar abgegrenzt, und es lässt sich nicht eindeutig feststellen, ob jemand, der ein personenbezogenes Datum erhebt oder verwendet, damit in diesen Rechtskreis eingreift.

Irrwege der Rechtsentwicklung

Wohin diese Unklarheit führt, zeigen die Fälle unsinniger Berufung auf Datenschutz. Schon erwähnt ist das Urteil des Landgerichts Lüneburg in Sachen „unerwünschte Werbung".[258] Unverständlich ist es auch, dass sogar die Spendenwerbung gemeinnütziger Organisationen behindert wird – so geschehen dadurch, dass ein Rechtsanwalt versuchte, einer solchen Vereinigung die Verwendung seiner E-Mail-Adresse verbieten zu lassen, die er selbst veröffentlicht hatte (das Amtsgericht wies diese Klage mit Aplomb ab, und der Gesetzgeber hat die Spendenwerbung inzwischen erleichtert).[259] Geradezu gemeinschädlich wirkt es, wenn die Methode der Videoabstandsmessung, mit der die Polizei im Straßenverkehr die schlimmsten Rowdies dingfest machen kann, für verfassungswidrig erklärt wird – so geschehen in Österreich, wo der Verfassungsgerichtshof einen Verfassungsverstoß feststellte, weil eine genaue Gesetzesbestimmung über die Methode der Geschwindigkeits- und Abstandsmessung fehlte.[260]

258 S. oben S. 67 f.

259 Amtsgericht Köln, Urteil v. 30.1.2007, Az. 120 C 488/06 (unveröff.). Es heißt dort u.a. sehr zutreffend: „Der Kläger macht sich die Chancen der Internet-Technik zu nutze, indem er auf seiner Homepage ohne … Einschränkung zur Kontaktaufnahme einlädt. Es ist eine nicht vermeidbare Konsequenz, dass der Kläger damit zugleich auch E-Mails provoziert, für die er kein Interesse hat. Der Kläger kann diese Gefahr verringern, indem er seine E-Mail-Adresse lediglich an bereits akquirierte Kunden bekannt gibt." Ebenso Amtsgericht Hannover, Urteil v. 19.2.2003, 526 C 15759/02. Zur Spendenwerbung s. jetzt § 28 Abs. 3 Satz 2 Nr. 3 BDSG i.d.F.v. 14.8.2009.

260 Österreichischer Verfassungsgerichtshof, U. v. 9.2.2008, Az. 1944/07-09, www.vfgh.gv.at. S. a. dpa-Bericht in: Süddeutsche Zeitung v. 9.2.2008. Das Urteil zitiert seitenlang die Datenschutzbestimmungen in der Verfassung und im Gesetz, sagt aber nichts zu den kollidierenden Rechtspositionen. In dem entscheidenden Teil stützt es sich auf das Recht auf *Eigentum*, das durch die Anordnung einer Geldstrafe verletzt sei, weil für die Bestrafung eine verfassungskonforme (datenschutzrechtliche) Rechtsgrundlage fehle. Inzwischen ist die Gesetzeslücke geschlossen. Zu einer ähnlichen Entscheidung eines deutschen Gerichts s. Bull 2009.

Eine schwedische Staatsanwaltschaft leitete ein Strafverfahren gegen eine ehrenamtliche Mitarbeiterin einer Kirchengemeinde ein, weil sie auf eine von ihr eingerichtete Webseite für Konfirmanden Informationen über Kollegen aufgenommen hatte, die darüber nicht informiert und nicht einverstanden waren (Namen, z.T. nur Vornamen, Funktionen und bei einer Kollegin auch, dass sie sich am Fuß verletzt habe und krankgeschrieben sei). Als sich jemand beschwerte, löschte sie diese Informationen sofort. Das schwedische Gericht verurteilte sie trotzdem zu einer Geldstrafe von 4000 Kronen (ca. 465 Euro) – mit der Begründung, sie habe

> „personenbezogene Daten in einem automatisierten Verfahren verarbeitet, ohne dies zuvor der Datainspektion schriftlich gemeldet zu haben, sowie sensible personenbezogene Daten, nämlich über eine Fußverletzung und eine Teilkrankenschreibung, ohne Genehmigung verarbeitet" und „ohne Genehmigung verarbeitete Daten in ein Drittland übermittelt".

Mit diesen vermeintlich strafwürdigen Vorwürfen musste sich in zweiter Instanz das schwedische Berufungsgericht und auf dessen Vorlage hin der Europäische Gerichtshof befassen. Der fand es offensichtlich sehr interessant, in diesem Rahmen den Anwendungsbereich der Europäischen Datenschutz-Richtlinie genauestens zu klären, und in der Tat stellte er fest, dass die Internetveröffentlichung der Kirchengemeinde eine „automatisierte Datenverarbeitung" darstellte, auf welche die Richtlinie anzuwenden war – er fand aber einen Ausweg aus dieser beklemmenden Situation, indem er die schwedischen Richter aufforderte, zwischen der Äußerungsfreiheit der „Rechtsbrecherin" und der Privatsphäre der angegebenen Mitarbeiter abzuwägen und besonders zu berücksichtigen, dass sie den Interneteintrag auf den Widerspruch hin sogleich gelöscht hatte. Ein salomonisches Urteil – aber welch ein Aufwand für einen Rechtsstreit, der besser gar nicht begonnen worden wäre! Der Name Lindquist ist dadurch in die europäische Rechtsgeschichte eingegangen; denn er bezeichnet jetzt ein „wegweisendes" Urteil des EuGH.[261] An der Namensnennung in dem Urteil hat offenbar niemand Anstoß genommen.

Was not tut, ist eine Rückbesinnung auf die wesentlichen Ziele, die wir mit dem Rechtssystem „Datenschutz" verfolgen: Er soll das Persönlichkeitsrecht und andere Rechte des Individuums schützen. Es geht um Handlungs- und Entfaltungsfreiheit der Menschen, und der sorgsame Umgang mit den persönlichen Daten ist nur ein Mittel zum Zweck. Manche der Fragen, die heute unter datenschutzrechtlichen Aspekten erörtert werden, können und sollten besser unter den Titeln „Verbraucherschutz" und „unlauterer Wettbewerb" angegangen werden; dieser Ansatz ist viel praktikabler und sachnäher als die Vorschriften über die Sammlung, Übermittlung und Nutzung personenbezogener Daten.

261 Urteil v. 6.11.2003, Rs C-101/01, Entscheidungssammlung des EuGH 2003, I-12971; s. a. Siemen 2006, S. 267 ff.

Abgesehen davon ist die Vorstellung des Bundesverfassungsgerichts vollkommen unrealistisch, jeder könne frei über alle Daten verfügen, die ihn betreffen und die bereits bei anderen vorhanden sind. (Das Gericht konzediert deshalb auch sogleich, dass es Ausnahmen geben müsse.)[262] Zum Beweis der Irrealität der Selbstbestimmungs-Theorie brauche ich nicht einmal auf das Internet mit seinen Untiefen und „Bermuda-Dreiecken" zu verweisen, die nur wenige kennen. Der Versuch, sämtliche Daten zu lokalisieren, die zu einer Person online oder offline im Umlauf sind – damit jeder wissen kann, „wer was wann und bei welcher Gelegenheit" über ihn weiß (so die berühmte Formulierung im Volkszählungs-Urteil[263]), wäre von vornherein aus technischen Gründen und wegen des gewaltigen Aufwandes zum Scheitern verurteilt. Selbst wenn man nur die wichtigsten Datensammlungen berücksichtigen wollte, wäre ein riesiger Aufwand nötig, und der Nutzen wäre gering.

Manche Datenschützer halten es – Kulturpessimisten, die sie sind – für geboten, die Nutzung der Computer und des Internets insgesamt zu beschränken, sozusagen das Volumen der Technikanwendung zu limitieren. Dazu haben sie das Prinzip der „*Datensparsamkeit*" oder „*Datenvermeidung*" erfunden, das sogar in das Bundesdatenschutzgesetz (§ 3 a) eingefügt worden ist: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen". Das ist schlicht anachronistisch und von übermäßiger Angst vor der Technik geprägt. Im folgenden Satz dieses Paragraphen wird deutlich, was wirklich gemeint ist und was in bestimmten Fallgruppen sinnvoll ist, nämlich dass personenbezogene Daten möglichst anonymisiert oder pseudonymisiert werden sollen („soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert"). Im Normalfall ist „Datendiät" weder nötig noch sinnvoll; denn die Speicherung und Verarbeitung kann datenschutzgerecht so gestaltet werden, dass niemand auf die erforderliche „Nahrung" verzichten muss.

Es gilt, die weitere *Bürokratisierung* zu verhindern, die durch ein Übermaß an Datenschutznormen droht. Dass das Datenschutzrecht so *kompliziert* geworden ist, stellt die notwendige und unausweichliche Konsequenz des Volkszählungs-Urteils dar, wonach jede Ausnahme von der Selbstbestimmung über die „eigenen" Daten einer gesetzlichen Grundlage bedarf. Wenn jeder noch so harmlose Vorgang der Sammlung, Verarbeitung oder Verwertung personenbezogener Daten vom Gesetzgeber ausdrücklich „erlaubt" werden muss, können die Gesetze nicht mehr übersichtlich und kurz sein. Sie müssen so ausfallen, wie inzwischen viele von ihnen ausfallen: Vorschriften über die Zulässigkeit des Sammelns und Verwendens

262 BVerfGE 65, 1 (43 f.).
263 BVerfGE 65, 1 (43).

von Informationen, die sich über viele Seiten des Gesetzblatts erstrecken, vielschichtige Gebäude aus Grundsatznormen, Einzelermächtigungen, Ausnahmen und Gegenausnahmen, dazu Verfahrensvorschriften und Informationspflichten der Anwender sowie subjektive Rechte der Betroffenen. Der normale Computer- und Internet-Nutzer kann die Fülle der Vorschriften gar nicht kennen, geschweige denn beachten. Die Ausnahmen für private oder familiäre Informationsverarbeitung[264] reichen offensichtlich nicht weit genug; die Belastungen für kleine Unternehmen und Freiberufler können erheblich sein. So kommt es dazu, dass das an sich geltende Datenschutzrecht bei der Internetnutzung kaum noch beachtet wird.[265]

Jetzt rächt sich der Ehrgeiz der deutschen Datenschützer (zu denen ich anfangs ebenfalls gehört habe), das Informationswesen in Staat und Wirtschaft möglichst umfassend und lückenlos zu regeln. Andere Länder haben sich auf die besonders wichtigen Fallgruppen konzentriert, wir wollten „Omnibus-Gesetze". Während der Datenschutz in den USA nur punktuell eingeführt wurde (und daher mit Recht als lückenhaft angesehen wird), ist in Deutschland (und unter dem Einfluss deutscher Experten und der EU-Verwaltung auch in anderen europäischen Staaten) ein dichtes Regelwerk entstanden, mit dem die Bürger nicht wirklich vertraut werden können. Trotzdem ist die Anwendung der Datenschutzvorschriften oft umstritten; die vielen Generalklauseln weisen den Weg zu akzeptierbaren Entscheidungen nur sehr grob, zur Lösung der Interessenkonflikte steht in den Vorschriften zu wenig Substanzielles.

Wenn der Gesetzgeber aber alle nur in Betracht kommenden Besonderheiten der Informationsverarbeitung selbst konkret regeln und dabei immer „mehr" Datenschutz für „alle" will, ohne zwischen alltäglichen, harmlosen Vorgängen und schwerwiegenden Risiken für hochwertige Rechtsgüter zu unterscheiden, wuchern die Gesetze immer weiter.

Heute ist die Datenschutz-Diskussion in einer Sackgasse angelangt: Alle Bemühungen, den Schutz des Persönlichkeitsrechts und anderer wichtiger Interessen der Betroffenen zu verbessern, laufen auf neue rechtliche Regelungen hinaus, die den Umgang mit personenbezogenen Daten erschweren, also den Bestrebungen nach „Normenkontrolle" und „Entbürokratisierung" zuwiderlaufen. Die Forderung

264 Natürliche Personen sind nach dem BDSG (§ 2 Abs. 4 und § 3 Abs. 7) grundsätzlich verantwortliche „nicht-öffentliche Stellen"; von der Geltung des Gesetzes ausgenommen sind sie nur, wenn die Erhebung, Verarbeitung oder Nutzung der Daten „ausschließlich für persönliche oder familiäre Tätigkeiten" erfolgt (§ 1 Abs. 2 Nr. 3 a.E.). Der Entwurf einer EU-Datenschutz-Grundverordnung macht die Ausnahme davon abhängig, dass „ausschließlich persönliche oder familiäre Zwecke ohne jede Gewinnerzielungsabsicht" vorliegen (Art. 2 Abs. 2 Buchst. d).

265 Dazu meint Heller, „genau dieses Vollzugsdefizit" mache den Datenschutz „erträglich"; „ein ganz und gar verwirklichter Datenschutz" würde totale Überwachung bedeuten, also eine perfekte paternalistische Fürsorge, die das Internet entscheidend verändert (Heller 2012, S. 92 f.).

nach „mehr Datenschutz“ wird in den meisten Fällen undifferenziert und ohne Abwägung mit den Interessen derer erhoben, die legitimerweise Daten verwenden wollen. Die Verständigungsprobleme zwischen der Öffentlichkeit, die sich kritisch versteht, und den Betreibern und Nutzern von Datentechnik sind erheblich. Vielfach wird statt einer überlegten Fortentwicklung der gesetzlichen Instrumente nur eine Politik der öffentlichen *Gefühlspflege* gefordert – man will das diffuse Gefühl einer ängstlichen Öffentlichkeit bekämpfen, durch die Technik bedroht zu sein, obwohl diese Bedrohung eben nicht immer und überall besteht.

Trotz allem: Reformansätze

Die verfahrene Situation begründet aber auch eine Chance, nämlich die einer *Konzentration der Kräfte* auf die wesentlichen Fragen des Individualrechtsschutzes. Die Weichen müssen neu gestellt, die Kräfte auf die wirklich wichtigen Bereiche gerichtet werden. Praktisch bedeutet das vor allem die *Abkehr vom Verbotsprinzip*. Der oberste Grundsatz des Bundesdatenschutzgesetzes – dass nämlich die Verarbeitung personenbezogener Daten stets und überall nur zulässig sein soll, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG) –, führt in die Irre und verursacht eine Gesetzesflut ohnegleichen. Die EU-Kommission verstärkt diese Tendenz noch, indem sie mit dem Entwurf einer Datenschutz-„Grundverordnung“ die bisherigen Regelungsbemühungen auf ihre höhere Stufe hebt und das geltende Datenschutzrecht perfektionieren will, was eine neue Qualität von Bürokratisierung verursachen wird. Nach der Ansicht des früheren sächsischen Datenschutzbeauftragten Thomas Giesen würde eine europäische Datenschutzordnung „unser gesamtes Dasein reglementieren“.[266]

Die grundsätzliche Umkehr muss darin bestehen, dass wir nicht mehr sagen: Was nicht erlaubt ist, ist verboten! Der geltende Zentralsatz des Datenschutzrechts (§ 4 Abs. 1 BDSG) scheint ja eben dies zu verkünden – gegen alle Praxis der Informationsgesellschaft. Es muss lauten: *Was nicht verboten ist, ist erlaubt* – und damit wird ein großer Teil der Datenschutzvorschriften obsolet, nämlich die meisten derjenigen, die den Umgang mit Daten (Sammeln, Nutzen, Übermitteln, Verändern usw.) erst *zulassen*.[267] Wir können auf sie verzichten, wenn wir statt dessen diejenigen Handlungen *verbieten* oder unter Auflagen stellen, die aus der Fülle der Möglichkeiten als besonders riskant herausragen. Die Dekonzentration der Materie würde eine Konzentration auf die drängenden Fragen ermöglichen. Auch die Da-

266 Giesen 2012.

267 Demgegenüber plädiert Spindler 2012, S. 134 (These 17) für die Beibehaltung des „Verbots mit Erlaubnisvorbehalt“, „allerdings mit einem wesentlich erweiterten Erlaubnistatbestand für Internetveröffentlichungen und -kommunikationsbeziehungen“.

tenschutzbeauftragten würden davon profitieren, dass sie von unnötigen Prüfungen entlastet wären. Sie könnten mehr Einflussmöglichkeiten gewinnen, ohne ihr Personal weiter zu vermehren.

Während viele Datenschutz-Experten noch die Forderung erheben, das Datenschutzrecht durch Zusammenfassung, also Kodifikation, in eine adäquatere Form bringen zu können, wächst anderswo die Einsicht, dass wir die eigentlichen Probleme nur noch durch bereichsspezifische Regelungen in den Griff bekommen, die als Elemente der jeweiligen besonderen Rechtsmaterien und der entsprechenden Fachpolitik entwickelt und angewendet werden müssen. Es wird kein Datenschutzgesetzbuch analog dem Bürgerlichen Gesetzbuch, dem Handelsgesetzbuch oder dem Strafgesetzbuch geben, sondern zunehmend den Datenschutz betreffende Normen im BGB, HGB, StGB und in vielen Einzelgesetzen. Nur so wird es gelingen, die Interessen an Privatheit und Geheimhaltung mit den entgegenstehenden Interessen an Offenlegung und Transparenz vereinbar zu machen.

In diesem Sinne plädiert Kai von Lewinski mit konkreten Beispielen für die *Dekonzentration* des Datenschutzrechts auf die verschiedenen materiellen Rechtsbereiche.[268] Es bietet sich z.B. an, den datenschutzrechtlichen Verbraucherschutz in das Bürgerliche Gesetzbuch, die Vorschriften über das Scoring (§ 28 b BDSG) in das Kreditwesengesetz und den Datenschutz für den öffentlichen Bereich in das Verwaltungsverfahrensgesetz einzuordnen und für den Arbeitnehmerdatenschutz ein eigenständiges Gesetz zu erlassen[269] (ein gesetzlich geregeltes Arbeitsvertragsrecht gibt es nur in Ansätzen im BGB). Allerdings muss sich auch das Bundesverfassungsgericht von seiner bisherigen Linie absetzen, wonach fast jede Form des Umgangs mit personenbezogenen Daten einen „Eingriff" in das „informationelle Selbstbestimmungsrecht" darstellt; dieses Dogma (aus dem Volkszählungsurteil) hat wesentlich dazu beigetragen, dass ständig neue Gesetze über die Sammlung und Nutzung von Daten beschlossen werden mussten.

Die Gesamtzahl der Normen braucht bei dieser Strategie nicht weiter zu wachsen. Die wenigen Grundsätze, die allgemein gelten müssen, können vor die Klammer gezogen werden, also in einem deutlich verkürzten BDSG und entsprechenden Landesdatenschutzgesetzen komprimiert werden. Der Frankfurter Rechtsanwalt Ulrich Wuermeling hat jüngst vorgeschlagen, nur noch vier allgemeine Grundsätze auf alle Formen der Datenverarbeitung anzuwenden, nämlich: Datensicherheit, Auskunftsrecht der Betroffenen, Berichtigungsanspruch und Recht zum Widerspruch gegen die Nutzung persönlicher Daten zu Werbezwecken. Im Übrigen sollten nur Vorschriften für solche Datenverarbeitungen erlassen werden, die „über-

268 Lewinski 2011 b.
269 Lewinski 2011 b, S. 121.

wiegende schutzwürdige Interessen im Hinblick auf die Privatsphäre der betroffenen Personen berühren". [270]

Eine Kodifikation wäre zwar rechtsästhetisch schöner als die Aufsplitterung der Materie auf viele Einzelgesetze. In dem Moment, in dem die verschiedenen Ressorts ihre „eigenen" Datenschutzgesetze machen, verliert überdies das Querschnittswissen der Datenschutzexperten an Bedeutung. Aber die inhaltliche Qualität der Normen wird wachsen, wenn die für die jeweilige Materie Kompetenten auch dafür verantwortlich sind, wie mit den notwendigen Daten umgegangen werden darf. Die Federführung für den datenschutzrechtlichen Verbraucherschutz muss beim Verbraucherschutzministerium liegen, die für den Arbeitnehmerdatenschutz beim Arbeitsministerium usw. usw.

Einzelfragen, um die gestritten werden kann, bleiben freilich in reichem Maße erhalten. So ist es eine äußerst schwierige Aufgabe, die Fälle abzugrenzen, in denen eine *Einwilligung* der Betroffenen genügen soll, um die Datensammlung oder -nutzung zulässig zu machen. In einem großen Teil der gegenwärtigen Einwilligungstatbestände sucht man vergeblich nach der Freiwilligkeit der Einwilligung – die Geschäftsbedingungen, in die man bei dieser Gelegenheit einwilligen soll, sind kaum verständlich, und sie sind stets einseitig vorgegeben; die Nutzer haben selten eine Alternative, und die Behörden schaffen es selten, Änderungen herbeizuführen. Da ist es meist angebracht, statt der Einwilligungslösung eine gesetzliche Regelung zu schaffen. In manchen Fällen dürfte auch die Widerspruchsmöglichkeit angemessen sein;[271] sie wird zu Unrecht von manchen Experten verworfen.

Spezialrecht für das Internet?

Aber sind nicht all diese Überlegungen doch noch viel zu fern von dem Thema „Internet"? Brauchen wir nicht spezielle Regelungen gerade für diese Sphäre der ungeordneten Techniknutzung und für die dort auftretenden Nutzungskonflikte? Ja, das ist ein richtiger Ansatz, denn es ist ein neuer, bisher nicht hinreichend beachteter Tatbestand, dass sich jeden Tag Millionen Menschen ins Netz „versenken" und unzählige Informations- und Kommunikationsvorgänge auslösen. Diese können mit den herkömmlichen Vorschriften nicht richtig und gerecht beurteilt werden. Gerade hier zeigt sich, dass es ein vergebliches Unterfangen ist, alle diese Vorgänge erst einmal auf ihre Zulässigkeit zu prüfen. Das „Verbot mit Erlaubnisvorbehalt" erweist sich hier als juristische Kulisse, die nichts mehr mit der Wirk-

270 Entwurf einer Handlungsempfehlung, vorgetragen auf der Datenschutz-Konferenz des BMI und des Humboldt-Instituts für Internet und Gesellschaft (s. oben Fn. 234).

271 So nach Spindler 2012, S. 134 These 21, für Geodaten-Dienste (z.B. Google Street View).

lichkeit gemeinsam hat, und die verschiedenen formalen Pflichten werden von den Betreibern und Nutzern unzulänglich oder gar nicht erfüllt.[272]

Ein Teil der Internet-Gemeinde hat inzwischen bemerkt, dass man von einem verstärkten Datenschutz nicht immer mehr Freiheit, sondern jedenfalls auch lästige Einschränkungen zu erwarten hätte. Denn:

> „Nimmt man die deutschen Datenschutzgesetze zum Maßstab, dann sind nicht nur Facebook und Google Datenverbrecher, sondern Unmengen kleiner Blog-, Foren- und Homepagebetreiber. Wer von ihnen hat schon eine rechtlich einwandfreie Datenschutzerklärung auf seiner Website, wie sie das Telemediengesetz fordert? Wer schaltet ihr schon die geforderten Warnungen und Einverständnisabfragen vor, dass beim Ausliefern des Seiteninhalts Daten des Besuchers verarbeitet werden?“[273]

Durch strengere Regeln und strengere Aufsicht lässt sich das „Vollzugsdefizit“ nicht beseitigen. Die Vorschriften sind auf Unternehmen mit Organisationskapazität zugeschnitten, nicht auf „Gelegenheitstäter“ und andere Internetfreaks, die ohne Erwerbsabsicht handeln, z.B. „Produtzer“ im Sinne von Axel Bruns.[274]

Andererseits wäre es ebenso falsch, ein umfassendes neues Recht für das Internet schaffen zu wollen. Wenn es richtig ist, dass im Internet nicht erlaubt sein kann, was offline verboten ist, wenn also online die gleichen Maßstäbe gelten, dann besteht die rechtspolitische Aufgabe darin, die angemessenen rechtlichen Formen zu finden, also die vorhandenen Rechtsinstitute auf die neuen tatsächlichen Phänomene zu erstrecken bzw. an sie anzupassen. Der erste Satz, nein der „Vorspann“ oder „Hintergrund“ eines solchen Regelwerks müsste sein: Der Austausch von Informationen und Meinungen über das Netz ist frei. Es wäre ein Anachronismus, das Einstellen von Texten oder Bildern in das Internet und die Kommunikation über das Netz von einer Erlaubnis abhängig zu machen; es geht schon zu weit, jeweils eine Rechtfertigung für die Internetnutzung vorauszusetzen (was ja bedeuten würde, dass der Nutzer gegenüber einer Behörde begründen muss, warum er oder sie etwas kommuniziert – eine eindeutig freiheitswidrige Belastung). Nur die *Grenzen* der Internetnutzung müssen rechtlich festgelegt sein, die aus dem Schutz kollidierender Rechte resultieren, also u.a. der Persönlichkeitsschutz.

Einen ersten Versuch, den Persönlichkeitsschutz im Internet zu stärken, hat das Bundesinnenministerium bereits unter dem seinerzeitigen Minister Thomas de Maizière unternommen. Er hat einen Vorschlag erarbeiten lassen,[275] der an die einschlägige Rechtsprechung des Bundesgerichtshofs und des Bundesverfassungs-

272 Nachweise zu Facebook etwa bei Weichert 2012, S. 250. S. a. oben S. 34 f.
273 Heller 2011, S. 82.
274 Internetnutzer, die zugleich Inhalte produzieren (Bruns 2009).
275 Entwurf v. 1.12.2010. Dazu Bull 2011 b.

gerichts anknüpft. Bei kleinen Differenzen (in Bezug auf die Bindung der Medien) wird diese langjährige Judikatur überwiegend als angemessen betrachtet. Ein vollständiger Neuansatz wäre weder nötig noch sinnvoll. Das allgemeine Persönlichkeitsrecht schützt den Einzelnen bereits jetzt nicht nur in der realen Welt vor Verleumdung, Beleidigung und anderen Beeinträchtigungen; es kann so weiterentwickelt werden, dass die neuen Phänomene der Internetnutzung adäquat erfasst werden. Der Innenminister wollte mit seinem Entwurf nur die *„rote Linie"* festlegen, die bei der Internetnutzung nicht überschritten werden darf; diese „rote Linie" besteht in dem Verbot, personenbezogene Daten in Telemedien zu veröffentlichen,

> „wenn dadurch ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen herbeigeführt wird, … soweit nicht eine andere Rechtsvorschrift dies erlaubt oder anordnet oder ein überwiegendes schutzwürdiges Interesse an der Veröffentlichung besteht".

Das ist eigentlich selbstverständlich und könnte auch ohne ausdrückliche gesetzliche Regelung von den Gerichten so entschieden werden. Interessant und weiterführend ist aber der folgende Satz:

> „Ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen liegt insbesondere vor, wenn in Telemedien personenbezogene Daten veröffentlicht werden,
>
> 1. die geschäftsmäßig gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet wurden und die dadurch ein umfangreiches Persönlichkeits- oder Bewegungsprofil des Betroffenen ergeben können oder
> 2. die den Betroffenen in ehrverletzender Weise beschreiben oder abbilden".

Als weitere Beispiele für verbotene Veröffentlichungen sind in der Mitteilung über den Entwurf genannt: die Veröffentlichung von Telekommunikations-Verbindungsdaten, die Offenlegung von Betreuungsverhältnissen und das systematische Veröffentlichen des Aufenthalts- und Wohnorts von vorbestraften Personen. Für bestimmte Internetdienste – Gesichtserkennungsdienste, Profilbildungen anhand von Suchmaschinen und Erhebung von Standortdaten – sind spezielle Regelungen vorgesehen.

Bemerkenswert (und begrüßenswert) ist, dass hier nicht die Datenspeicherung oder -verarbeitung, sondern die *Veröffentlichung* von Daten geregelt wird. Darin liegt eine Abkehr von dem Denken in *möglichen* Risiken, hin zu den *wahrscheinlichen* Bedrohungen von Individualrechten. In den sozialen Netzwerken werden die Daten ohnehin überwiegend mit Zustimmung der Betroffenen gespeichert; es dürfte kaum gelingen, die Entwicklung dieser Medien von Vorschriften des nationalen Rechts abhängig zu machen, mit denen die Zulässigkeit der Datenspeiche-

rung eingeschränkt werden soll. (Das Land Schleswig-Holstein versucht dies gleichwohl; nach einer Novelle zum Landesdatenschutzgesetz ist die Veröffentlichung von Daten im Internet nur zulässig, wenn „diese Form der Veröffentlichung durch eine Rechtsvorschrift erlaubt ist oder der Betroffene in diese Form eingewilligt hat“. Die Veröffentlichung ist überdies auf höchstens fünf Jahre zu befristen.[276])

An dem Entwurf des Bundesinnenministeriums fällt positiv auf, dass nicht jede Auswertung personenbezogener Daten als „gefährlich“ angesehen wird, so dass das Veröffentlichungsverbot nur das „geschäftsmäßige“ Handeln erfasst – und auch dies nur dann, wenn ein „umfangreiches Persönlichkeits- oder Bewegungsprofil des Betroffenen“ dabei herauskommen kann. „Profile“ sind nicht immer missbrauchsanfällig; wollte man sie gänzlich verbieten, so würde man auch vernünftige und notwendige Nutzungsweisen ausschließen.

Dieser BMI-Entwurf ist nicht vollständig und nicht in allen Details ausgereift. Er erscheint manchen als zu knapp und anderen vielleicht schon als zu differenziert. Er ist aber leider nicht intensiv diskutiert worden. Es wäre schade, wenn er unerörtert in der Schublade verschwände.

Die EU-Datenschutz-„Grundverordnung“: eine Autobahn zur Bürokratisierung

Die EU-Kommission hat im Januar 2012 den Entwurf einer Datenschutz-Verordnung veröffentlicht, der auf einen Schlag das gesamte nationale Datenschutzrecht beiseite zu schieben scheint.[277] In 91 Artikeln, die teilweise mehr als eine Druckseite füllen, versucht die EU-Kommission den Datenschutz zu perfektionieren und in ganz Europa auf ein einheitliches Niveau zu heben. (Die bisher geltende Datenschutz-Richtlinie hat nur 34 – auch schon recht umfangreiche – Artikel.) Wer den Entwurf zum ersten Mal liest, wird vielleicht zu dem Urteil gelangen, es handle sich um eine ganz ausgezeichnete Zusammenfassung und Weiterentwicklung aller bisherigen nationalen und supranationalen Normen über den Datenschutz. Die grundlegenden Prinzipien und die jeweils notwendigen Ausnahmen sind sorgfältig zusammengetragen und in eine sinnvolle Ordnung gebracht, und die Verordnung scheint einen einheitlich hohen Standard des Datenschutzes in ganz Europa anzustreben.

Allerdings ändert sich diese Beurteilung, wenn man sich vergegenwärtigt, dass bisher in Europa ein Flickenteppich nationaler Datenschutzgesetze gilt und es einer Sisyphusarbeit gleichen dürfte, diese Rechtslage auf der Grundlage der EU-Ver-

276 LDSG SH i. d. F. v. 11.1.2012, GVOBl. S. 78. S. a. Landtags-Drs. 17/1698 und 17/2076.
277 KOMM (2012) 11 endgültig v. 25. 1. 2012. Aus der Lit. dazu u.a.: von Lewinski 2012; Roßnagel 2012. S. a. oben S. 30 f.

ordnung tatsächlich zu vereinheitlichen. Eine EU-Verordnung ist ebenso verbindlich wie ein Gesetz, sie lässt den Mitgliedstaaten – anders als die geltende Datenschutz-Richtlinie der EG – keinen Spielraum zu eigenen Entscheidungen darüber, *wie* das vorgegebene Ziel zu erreichen sei. Das Unternehmen, das gesamte Datenschutzrecht zu „vergemeinschaften", ist denn auch schon auf Widerspruch aus dem Bundesverfassungsgericht gestoßen: Das oberste nationale Gericht fürchtet offenbar, dass seine wirkungsmächtige Rechtsprechung zum „informationellen Selbstbestimmungsrecht" und seinen Auswirkungen auf die deutsche Gesetzgebung und Verwaltung mit dieser EU-Verordnung von Brüssel mit einem Schlag über den Haufen geworfen wird.[278]

Diese Sorge ist vielleicht etwas übertrieben; es wird zumindest einige Zeit dauern, ehe die gewichtige Tradition der datenschutzrechtlichen Verfassungsjudikatur unter dem Einfluss des europäischen Rechts ausläuft. Aber aus einem anderen Grunde dürfte eine solche Verordnung tatsächlich erhebliche Probleme aufwerfen. Der Text ist nämlich so gehaltvoll und komprimiert, aber auch so abstrakt, dass seine Anwendung unzählige Streitfragen aufwerfen wird, und das ist strukturell begründet: In dem Bestreben, alle nur in Betracht kommenden Fälle von Datenverarbeitung zu erfassen, werden notwendigerweise sehr weite und vieldeutige Formulierungen gewählt. Spezialisierte Rechtsanwälte werden sich über viele neue Mandate freuen, aber auch sie werden ihren Mandanten oft keine klare Auskunft geben können, was denn nun rechtens ist und was nicht.

Denn der entscheidende Mangel des Verordnungsentwurfs ist: Es fehlt an einem Kompass, der die Richtung bestimmt. Die Prinzipien, nach denen sich die Rechtmäßigkeit der Verarbeitung richten soll, müssen gegeneinander abgewogen werden, aber die Verordnung sagt nicht, wie das geschehen soll. In der grundlegenden Norm des Artikel 1 steht neben dem Ziel „Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Rechts auf Schutz von personenbezogenen Daten" auch das entgegengesetzte Ziel „sicherzustellen, dass der freie Verkehr personenbezogener Daten innerhalb der Europäischen Union aus Gründen des Schutzes von Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten wird" – also eine von Anfang an in sich widersprüchliche Zielsetzung!

Der hohe Datenschutzstandard, den die EU-Kommission mit ihrem Vorschlag anstrebt, kann schon deshalb nicht erreicht werden, weil die Datenverarbeitung nach dessen einschlägiger Vorschrift (Art. 6) fast immer für rechtmäßig erklärt werden wird; andernfalls wird man darüber streiten, also ebenfalls keine strengeren Maßnahmen treffen. Dieser Artikel nennt sechs Rechtmäßigkeitsgründe: von der Einwilligung des Betroffenen bis zur „Verwirklichung" eines „berechtigten Inter-

278 Vgl. Masing (Richter des Bundesverfassungsgerichts) 2012 a. Dagegen jedoch verschiedene Leserbriefe von Europarechts-Experten in der SZ v. 25. 1. 2012.

esses“ des Verantwortlichen. Alle diese Erlaubnisklauseln sind so formuliert, dass erst eine sorgfältige Auslegung und Abwägung zu dem Ergebnis „rechtmäßig“ oder „nicht rechtmäßig“ führt. Über jede dieser Formulierungen kann man trefflich streiten. Nach der längsten dieser Klauseln (Art. 6 Abs. 1 Buchstabe f) ist die Datenverarbeitung rechtmäßig, wenn sie

> „zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich“ ist, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt“.

Die Entwurfsverfasser hielten es offenbar für unmöglich, Konfliktbereiche durch klare Regeln zu befrieden: so haben sie statt der benötigten Lösungen abstrakte Vorüberlegungen zum Norminhalt erhoben.

Das hat u.a. zur Folge, dass kaum ein Prinzip, das in dem Entwurf enthalten ist, ohne Ausnahme bleibt. So bringt zwar – was neu und an sich begrüßenswert ist – der Artikel über „Recht auf Vergessenwerden und auf Löschung“ einen Anspruch auf Löschung auch solcher Daten, die man ursprünglich selbst in das Netz eingegeben hat. Man soll also seine Einwilligung in die Verarbeitung zurückziehen können (Art. 17 Abs. 1 Buchstabe b). Darüber hinaus sollen u.a. alle Daten, die für die ursprünglichen Zwecke nicht mehr erforderlich sind, gelöscht werden (ebd. Buchstabe a). Verweise auf gelöschte Daten sollen möglichst aus allen Suchdiensten entfernt werden (Art. 17 Abs. 2). Aber sogleich folgen – notwendigerweise! – Ausnahmen von der Löschungspflicht, etwa

> „zur Erfüllung einer gesetzlichen Pflicht zur Vorhaltung der personenbezogenen Daten, der der für die Verarbeitung Verantwortliche nach dem Unionsrecht oder dem Recht eines Mitgliedstaats unterliegt, wobei das mitgliedstaatliche Recht ein im öffentlichen Interesse liegendes Ziel verfolgen, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel stehen muss“ (Art. 17 Abs. 3 Buchstabe d).

Wer kann das verstehen? Wie kann man Klarheit und Verlässlichkeit des Rechts erwarten, wenn die Rechtsanwender erst einmal prüfen sollen, ob eine gesetzliche (!) Speicherungsverpflichtung etwa nicht dem „öffentlichen Interesse“ entspricht und ob das nationale Recht etwa „das Wesen des Rechts auf den Schutz personenbezogener Daten“ missachtet und in einem unangemessenen Verhältnis zu dem verfolgten Zweck steht. Der Datenverarbeiter würde damit zum Richter über den Gesetzgeber; denn der hätte seine wesentliche Pflicht verletzt, wenn er ein Gesetz erlassen hätte, das dem Gemeinwohl widerspricht! Und was das „Wesen“ des Da-

tenschutzes ausmacht, müssten die Verfasser der EU-Verordnung auch dies eigentlich besser wissen als die Adressaten. Es ist ein Armutszeugnis des Verordnunggebers, wenn hier statt einer eindeutigen Regelung auf eine rechtstheoretische Idee verwiesen wird.

Unser deutsches Datenschutzrecht ist – bei aller Kritik, die auch an ihm geübt werden kann – wesentlich besser ausgeformt, und auch andere EU-Staaten haben durchdachte und effektive Datenschutzgesetze. Der Versuch, den Mitgliedstaaten ein materiell einheitliches Datenschutzrecht durch eine EU-Verordnung aufzunötigen, wird nicht gelingen. Die Rechtsordnungen werden auch ohne diesen verbindlichen Rechtsakt weiter zusammenwachsen, so wie es schon bisher im Rahmen der Datenschutz-Richtlinie geschehen ist (die nur in den Zielen, nicht in der Einzelumsetzung verbindlich ist). Bestimmte Fragen – etwa die Verwendung von Kundendaten – können durch spezielle Vorschriften einheitlich geregelt werden, aber den Ehrgeiz einer allumfassenden Normierung sollte die EU fallen lassen.

Im Übrigen sollte die EU sich darauf beschränken, die Durchsetzung eines einheitlichen Datenschutzniveaus durch Verfahrensregeln und verstärkte Auskunfts- und Benachrichtigungsrechte der Betroffenen zu unterstützen. Der Verordnungsentwurf enthält dazu einige wichtige Ansätze. Insbesondere die Regeln über die Zuständigkeit der Aufsichtsinstanzen und Gerichte können den Betroffenen helfen, ihre Rechte wirksam zu verfolgen. Es würde danach immer noch schwierig bleiben, die „Giganten" der Szene wie Facebook und Google zur Einhaltung der Regeln zu zwingen, aber es wäre einfacher als ohne solche supra- und internationale Normen.

Die Fortsetzung der nationalen Datenschutzdebatte

Durch die EU-Initiative ist auch die Debatte über das deutsche Datenschutzrecht wieder angestoßen worden: Das nationale Recht kann nicht unverändert bleiben, wenn der europäische Rahmen sich ändert. Daraus hat das Bundesinnenministerium den richtigen Schluss gezogen, auch das BDSG zu überprüfen, und hat dazu Wissenschaftler und Praktiker aus dem In- und Ausland zusammengebracht. Auf einer internationalen Konferenz im Oktober 2012[279] sind die Fronten deutlich geworden, aber auch Wege aus der Sackgasse aufgezeigt worden. Wenn es eine Kernaussage der Konferenzmehrheit gab, dann war es diese: Es ist Zeit für die Konzentration auf das Wesentliche. Das Datenschutzrecht muss neu justiert werden, indem überflüssige Regeln abgebaut und die tatsächlich relevanten Risiken gezielter bekämpft werden. Die Abgrenzung ist nicht einfach, aber notwendig.

279 „Datenschutz im 21. Jahrhundert: Spielregeln für die Informationsgesellschaft", Berlin , 17./18. Oktober 2012, veranstaltet vom Bundesministerium des Innern und dem Alexander von Humboldt-Institut für Internet und Gesellschaft.

Stichworte dazu sind u.a.: Die *Auswertung* persönlicher Angaben ist „riskanter" als die bloße Sammlung und Speicherung, es kommt also auf die Art und Weise gerade der Auswertung an. Die Erstellung von *Profilen* ist häufig, aber nicht immer ein Anlass zur Aufmerksamkeit, jedenfalls wenn „*sensible"* Daten verwertet werden. Die *Heimlichkeit* der Informationsgewinnung spricht für strenge rechtliche Einbindung.

Der Regelungsbedarf erstreckt sich aber auch auf ganze Bereiche der Informationsverarbeitung, in denen regelmäßig Gefahren für Persönlichkeitsrechte und andere schützenswerte Interessen der Betroffenen bestehen: zu allererst bestimmte Anwendungen in den sozialen Medien (wobei aber eben nicht Verbote, sondern zielgerichtete Regelungen für die unerwünschten Verknüpfungen und Auswertungen angebracht sind), sodann u.a. Leistungskontrollen und Überwachung im Arbeitsverhältnis (ein Gesetzentwurf ist im Parlament anhängig), angemessene Verfahren der Kreditauskunfteien (ein Dauerthema), Verwaltung von Mitgliedschaftsdaten (Zweckentfremdungsverbot), Klärung von Zweifelsfragen um „Data Mining" und Direktwerbung, der Umgang mit Gesundheitsdaten und das „Internet der Dinge". Die Kunst der Gesetzgebung wird darin bestehen, die notwendige Präzision und Eindeutigkeit mit dem ebenso gebotenen Verzicht auf Bagatellregeln zu verbinden.

Manche Risiken, die im Ansatz bereits durch die Speicherung von Daten begründet werden, können in anderer Weise als durch den vorbeugenden Schutz der Daten ausgeräumt oder zumindest wesentlich vermindert werden, indem man nämlich – wie schon in den Vor-Datenschutz-Zeiten – bestimmte *Verwendungsweisen* einschränkt oder verbietet. Das heißt: Die guten alten Berufsgeheimnisse der Ärzte, Rechtsanwälte und Geistlichen und die vielfältigen Verschwiegenheitspflichten können als Vorbild für Verwertungsschranken dienen, ebenso die Zeugnisverweigerungsrechte der Journalisten und die Tilgungsregeln, die das Aufbewahren sensibler Daten erträglich machen, und die entsprechenden Verwertungsverbote – alles Instrumente eines „programmierten Vergessens". Schwierig und unsicher ist auch hier die Durchsetzung: Der Versuchung, gegen solche Pflichten zu verstoßen, unterliegen viele, darunter selbst Amtsträger aller Art und Journalisten.

Um es nochmals klar zu sagen: Es bedarf politischer Entscheidungen. Die Umsetzung der Regeln in technische Realisationen ist davon zu unterscheiden. Sofern die Technik-Verantwortlichen keine Umsetzungsmöglichkeiten erkennen, kann auch die Rechtspolitik nichts ausrichten, aber die Richtlinien müssen von den Entscheidungsbefugten kommen.

Die Verantwortung für Infrastruktur und Rechtsordnung der Internetwirtschaft

„Quer“ zu den Aufgaben der Fachpolitiken liegt als allgemeines Problemfeld das der Sicherheit des Netzes und unserer Abhängigkeit vom Netz. Es ist politisch weniger aufregend und kaum ein Thema für die Feuilletons, aber praktisch wahrscheinlich wichtiger als die meisten anderen Probleme rund ums Internet. Auch hier rückt die Verantwortung des Staates in das Zentrum der Aufmerksamkeit. Was lange verfemt war, ist heute wieder im Schwange: Statt die Wahrnehmung wichtiger Aufgaben der Privatwirtschaft zu überlassen, werden Politik und Verwaltung in die Pflicht genommen.

Der Ausbau und die Ausgestaltung des Internets sind allerdings, für sich genommen, nicht einmal politische Ziele, sondern in erster Linie Gegenstand von Marktprozessen. Es geht um Mittel und Prozesse zur leichteren Kommunikation und die Sicherung ihrer Funktionsfähigkeit. Das Netz ist kein Selbstzweck, aber es ist auch kein Werkzeug des Staates für seine Zwecke. Für die Netzpolitik folgt daraus: Nicht die weitere Verbesserung oder Beschleunigung der Technik steht an der Spitze der politischen Agenda, sondern unser Umgang mit ihr. Die Technik entwickelt sich ganz überwiegend „von selbst“, also aus den ökonomischen Potentialen und den Marktverhältnissen. Sie muss rechtlich eingebunden und eingegrenzt werden, damit sie menschengerecht genutzt werden kann; dazu sind klare politische Entscheidungen nötig. Aber sie bedarf kaum der Unterstützung der Bürger oder des Staates – abgesehen von den Anstößen und Hilfen zur Verbesserung der Infrastruktur, für die es eine Verantwortung des Staates gibt, weil sonst nicht garantiert wäre, dass jeder – auch die Bewohner dünn besiedelter Landesteile – den Zugang zu dem faszinierenden Kosmos des Netzes hat.

Unter diesen Umständen könnte man fragen, ob es denn angemessen sei, dass die *Infrastruktur* zu einem wichtigen Teil vom Staat vorgehalten oder gefördert wird. Die Antwort ist: Ja, der Staat soll den Ausbau des Übertragungsnetzes und der Stromversorgung unterstützen, damit möglichst alle Einwohner sich diskriminierungsfrei und zu erträglichen Konditionen anschließen können. Steuergelder sind dafür gut angelegt, auch wenn private Unternehmen darauf aufbauen und Gewinne machen. Nicht jede Form von Innovationsförderung ist angebracht; hier aber darf der Staat sich engagieren, und er soll es auch, zumindest wenn sonst Ungleichheiten entstehen. Die Unternehmen müssen jedoch zu diskriminierungsfreiem und wettbewerbsgerechtem Handeln angehalten werden.

In Deutschland kann die Bundesnetzagentur diese Verpflichtungen durchsetzen. Sie hat aufgrund des Telekommunikationsgesetzes gegenüber den Betreibern öffentlicher TK-Netze mit „beträchtlicher Marktmacht“ allerhand Befugnisse, z.B. anzuordnen, dass „Vereinbarungen über den Zugang auf objektiven Maßstäben beruhen, nachvollziehbar sein, einen gleichwertigen Zugang gewähren und den

Geboten der Chancengleichheit und Billigkeit genügen müssen".[280] Diese einfachgesetzliche Regulierung muss fortgeschrieben und ergänzt werden (Stichwort: Universaldienstleistungspflicht).[281]

Eine politisch unauffällige Abteilung der Netzpolitik befasst sich damit, den Rahmen der technischen Entwicklung weiter zu verbessern, indem technische Standards und sonstige einheitliche Vorgaben entwickelt und in technische Normen gefasst werden, Zusammenarbeit ermöglicht wird und gemeinsame Einrichtungen geschaffen werden. Die Informationsnetze von Bund, Ländern und Gemeinden müssen koordiniert, das „E-Government" weiter ausgebaut werden.[282] Die verfassungsrechtliche Legitimation zur Ebenen übergreifenden Zusammenarbeit beim Ausbau der Verwaltungsinformationssysteme ist seit 2009 vorhanden.[283] Die Diskussion über diese Entwicklungen wird fast ausschließlich unter Fachleuten aus Wirtschaft und Verwaltung geführt; für die Politik ist dieses Themenfeld unergiebig, weil nicht wahlwirksam. Gleichwohl verdienen auch diese Arbeitsfelder die Aufmerksamkeit der Öffentlichkeit, denn es geht nicht nur um hohe Investitionen aus Steuermitteln, sondern auch um den Stil und das Klima, in dem die Verwaltung sich mit den Angelegenheiten der Bürger befasst. Technokratisches und ökonomisches Denken genügt nicht; die Bürger haben Anspruch darauf, dass der Staat ihnen entgegenkommt – im wörtlichen wie im übertragenen Sinne.

Kontrolle oder Vertrauen

Nicht nur unter Liberalen und Linken ist Lenins Spruch beliebt, Vertrauen sei gut, aber Kontrolle sei besser. Lenin meinte die Kontrolle durch die führende Gruppe. Zur Demokratie gehört eine wirkungsvolle, durchsetzungsstarke Kontrolle staatlicher Machtausübung durch das Volk und seine Vertreter. „Gewaltenteilung" bedeutet heute – über die recht einfachen Vorstellungen von Montesquieu und der anderen frühen Theoretiker hinaus – ein System von Gewichten und Gegengewichten, Checks and Balances. Kennzeichnend für eine funktionierende Demokratie ist gerade auch, dass es außer den unabhängigen Gerichten noch besondere Kontrollinstanzen wie die Datenschutzbeauftragten, Wehrbeauftragten und weitere „Ombudspersonen" gibt, die ebenfalls in Unabhängigkeit über die Exekutive wachen.

280 § 19 Telekommunikationsgesetz. S. a. § 21 und § 30 (Entgeltregulierung).
281 S. schon oben S. 42.
282 Dazu besonders klarsichtig: Lenk 2004; weiterführend Brüggemeier/Dovifat u.a. 2006 sowie Brüggemeier/Lenk 2011.
283 Art. 91 c GG i.d.F. v. 29.7.20009, BGBl. I S. 2248. Vgl. dazu u.a. Seckelmann 2009 und Schulz 2010.

Und doch: Alle diese Institutionen – vom Parlament bis zur Polizeiwache – können ihre Aufgabe nur erfüllen, wenn den handelnden Personen ein Mindestmaß an Vertrauen entgegengebracht wird. Ohne Vertrauen in die Integrität und das Engagement derer, die für die Allgemeinheit handeln, kann auch die beste Verfassung nicht verwirklicht werden. Auch die Aufsichtsinstanzen bedürfen eines gewissen Vertrauens ihrer „Kunden", der Bürger; sonst lassen diese sie ins Leere laufen oder fordern eine Kontrolle über die Kontrolleure. Schlimmer noch: Wenn es an einem Grundvertrauen in die staatlichen Institutionen fehlt, kann auch das staatliche Recht nicht durchgesetzt werden. Dafür zahlen dann vor allem die Ärmeren, die sich keinen eigenen Schutz leisten können.

Mir ist bewusst, dass Ängste nicht durch rationale Argumente abgebaut und tiefsitzende Einstellungen nicht durch Gesetze geändert werden können.[284] Das notwendige Vertrauen kann nicht angeordnet oder durch staatliche Maßnahmen eingefordert werden. Es muss aus der Gesellschaft selbst erwachsen. Der Streit um die „digitale Bedrohung" wird auch durch noch so kluge Einsichten nicht allseits befriedigend beendet werden. Dennoch sollten wir nicht von dem Versuch ablassen, den Menschen solche Überlegungen zu vermitteln. Das Themenfeld, das sich hier auftut, ist überdies viel zu attraktiv, als dass es in absehbarer Zeit „erledigt" sein könnte. Immerhin: Wenn wir uns nicht mit Gemeinplätzen und Stammtischparolen begnügen, sondern die verfügbaren Erkenntnisse und Erfahrungen systematisch verarbeiten, können wir uns wohl den einen oder anderen Umweg ersparen.

284 Instruktiv Herrmann 2012.

Literaturverzeichnis

Ahlert, Christian 2001: ICANN als Paradigma demokratischer, internationaler Politik? Internetregulierung zwischen Technik und Demokratie, in: Holznagel/Grünwald/Hanßmann, S. 44

Altmaier, Peter 2011: Noch mehr Demokratie wagen, in. Frankfurter Allgemeine Zeitung v. 15.10.2011, S. 35

Barber, Benjamin R. 1998: Wie demokratisch ist das Internet?, in: Telepolis Heft 4-5, S. 4

Barber, Benjamin R. 2009: Which Technology for which Democracy?, in: Holznagel/Grünwald/Hanßmann S. 209

Beckedahl, Markus/Lüke, Falk 2012: Die digitale Gesellschaft. München

Behrens, Christoph 2011: Die Überwachungsmaschine, in: Süddeutsche Zeitung v. 1.12.2011

BfDI 2011: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 23. Tätigkeitsbericht 2009-2010. Bonn. Zugleich Bundestagsdrucksache 17/5200

Bieber, Christoph/Eifert, Martin/Groß, Thomas/Lamla, Jörn (Hrsg.) 2009: Soziale Netze in der digitalen Welt. Frankfurt am Main/New York

Bolz, Norbert 2010: Jeder ist seines Clickes Schmied, in: Süddeutsche Zeitung Wochenende v. 28./29.8.2010, S. V2/3

Borchardt, Alexandra 2011: Wir sind die Klicks, in: Süddeutsche Zeitung Wochenende v. 17./18.12.2011

Briegleb, Till 2011: Abstimmen für die Graburne. Demokratie oder Illusion? Zur Spielplan-Wahl am Thalia Theater, in: Süddeutsche Zeitung v. 21.12.2011

Brill, Klaus 2012: Netz gegen Politik, in: Süddeutsche Zeitung v. 8.2.2012

Brüggemeier, Martin/Dovifat, Angela/Kubisch, Doreen/Lenk, Klaus/Reichard, Christoph/Siegfried, Tina 2006: Organisatorische Gestaltungspotenziale durch Electronic Government: Auf dem Weg zur vernetzten Verwaltung. Berlin

Brüggemeier, Martin/Lenk, Klaus (Hrsg.) 2011: Bürokratieabbau im Verwaltungsvollzug: Better Regulation zwischen Go-Government und No-Government. Berlin

Bruns, Axel 2009: Produtzung: Von medialer zu politischer Partizipation, in: Bieber/Eifert/Groß/Lamla, S. 53

Bull, Hans Peter 1984: Datenschutz oder Die Angst vor dem Computer. München

Bull, Hans Peter 1999: Demokratie braucht Zeit – Zur Frage demokratischer Abstimmungen mittels telekommunikativer Verfahren, in: Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999. Heidelberg, S. 293

Bull, Hans Peter 2009: Sind Video-Verkehrskontrollen „unter keinem rechtlichen Aspekt vertretbar“?, in: Neue Juristische Wochenschrift, S. 3279

Bull, Hans Peter 2011 a: Informationelle Selbstbestimmung – Vision oder Illusion? 2. Aufl. Tübingen

Bull, Hans Peter 2011 b: Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, in: Neue Zeitschrift für Verwaltungsrecht, S. 257

Bull, Hans Peter 2011 c: Regulierung des Internets mit den Mitteln des Datenschutzes?, in: spw Heft 182, S. 21

Bull, Hans Peter 2011 d: Steuerpflicht, Sozialstaat und Freiheit des Individuums, in: Schliesky, Utz/Ernst, Christian/Schulz, Sönke E. (Hrsg.) 2011: Die Freiheit des Individuums in Kommune, Staat und Europa. Festschrift für Edzard Schmidt-Jortzig. Heidelberg, S. 465

Bull, Hans Peter 2012: Widerspruch zum Mainstream. Ein Rechtsprofessor in der Politik. Berlin

Determann, Lothar 1999: Kommunikationsfreiheit im Internet: Freiheitsrechte und gesetzliche Beschränkungen. Baden-Baden

DJT (Hrsg.) 2012: Thesen der Gutachter und Referenten zum 69. Deutschen Juristentag, München 2012

DIVSI (Hrsg.)) 2012: DIVSI-Milieu-Studie zu Vertrauen und Sicherheit im Internet. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet. Hamburg

Drösser, Christoph 2011: Von wegen vergessen, in: Die Zeit v. 27.1.2011, S. 33

Eberle, Carl-Eugen 2011: Netzneutralität – Determinanten und Anforderungen, in: Mehde, Veith/Ramsauer, Ulrich/Seckelmann, Margrit (Hrsg.), Staat, Verwaltung, Information. Festschrift für Hans Peter Bull. Berlin, S. 979

Von Eimeren, Birgit/Frees, Beate 2012: 76 Prozent der Deutschen online – neue Nutzungssituationen durch mobile Endgeräte, in: Media Perspektiven 7-8, S. 362

Eisel, Stephan 2011: Internet und Demokratie. Freiburg i.Br.

Emmer, Martin/Vowe, Gerhard/Wolling, Jens 2011: Bürger online. Die Entwicklung der politischen Online-Kommunikation in Deutschland. Konstanz

Esslinger, Detlef 2012: Das große Faseln. Warum die Aufregung über das Meldegesetz etwas absurd ist, in: Süddeutsche Zeitung v. 12.7.2012, S. 11

Europäische Kommission 2012: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012, KOM (2012) 11 endgültig

Fischermann, Thomas/Hamann, Götz 2011: Zeitbombe Internet. Warum unsere vernetzte Welt immer störanfälliger und gefährlicher wird. Gütersloh

Franda, Marcus F. 2001: Governing the Internet: The Emergence of an International Regime. Boulder, Colorado/London

Frisse, Juliane 2012: Gut gemeint, in: Süddeutsche Zeitung v. 27.2.2012

Gehlen, Dirk von 2011: Raubkopierer in die Parlamente!, in: Süddeutsche Zeitung v. 8.11.2011

Geiselberger, Heinrich (Red.) 2011: WikiLeaks und die Folgen: Netz – Medien – Politik. Berlin

Gelernter, David 2012: Hausfrauen, Polzisten – jeder ist als Lehrer geeignet, in: Frankfurter Allgemeine Zeitung v. 8.2.2012

Giesen, Thomas 2012: Demokratiewidrig: Die geplante EU-Verordnung zum Datenschutz würde unser gesamtes Dasein reglementieren, in: Süddeutsche Zeitung v. 18.5.2012

Görig, Carsten 2011: Gemeinsam einsam: Wie Facebook, Google & Co. unser Leben verändern, Zürich

Graff, Bernd 2012: Wir sind alle Urheber, in: Süddeutsche Zeitung v. 2.2.2012

Güntner, Joachim 2012: Das Unbehagen am Copyright, in: Neue Zürcher Zeitung v. 27.2.2012

Hamann, Götz 2011: Nützliche Vandalen, in: Die Zeit v. 29.12.2011

Härting, Nico 2005: Internetrecht. 2. Aufl. Köln

Han, Byung-Chul 2012: Transparenzgesellschaft. Berlin

Haug, Volker 2010: Internetrecht. 2. Aufl. Stuttgart

Heckmann, Dirk 2011 a: Smart Life – Smart Privacy Management. Privatsphäre im total digitalisierten Alltag, in: Kommunikation & Recht, H. 1, S. 1

Heckmann, Dirk (Hrsg.) 2011 b: Internetrecht, Telemediengesetz, E-Commerce, E-Government. Saarbrücken

Heller, Christian 2011: Post-Privacy: Prima leben ohne Privatsphäre. München

Herrmann, Sebastian 2012: Wie man Starrköpfe überzeugt, in: Süddeutsche Zeitung v. 1.2.2012

Heveling, Ansgar 2012: „Netzgemeinde, ihr werdet den Kampf verlieren!“, in: Handelsblatt v. 30.1.2012

Hoffmann-Riem, Wolfgang 2009: Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, in: Archiv des öffentlichen Rechts 134, S. 513

Hoffmann-Riem, Wolfgang 2012: Regelungsstrukturen für öffentliche Kommunikation im Internet, in: Archiv des öffentlichen Rechts 137, H. 4 (i.E.)

Hofmann, Niklas 2012: Ohne Netz keine Partizipation, in: Süddeutsche Zeitung v. 16.1.2012

Holznagel, Bernd/Grünwald, Andreas/Hanßmann, Anika 2001: Elektronische Demokratie: Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis. München

Holznagel, Bernd/Schumacher, Pascal 2011: Netzpolitik Reloaded: Pflichten und Grenzen staatlicher Inernetpolitik, in: Zeitschrift für Rechtspolitik, S. 74

Hornung, Gerrit/Fuchs, Katharina 2012: Nutzerdaten im Smart Grid – zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung, in: Datenschutz und Datensicherung H.1, S. 20

Jun, Uwe 2009: Liegt die Zukunft politischer Partizipation wirklich bei der „Produtzung“?, in: Bieber/Eifert/Groß/Lamla, S. 87

Kammer, Matthias/Huppertz, Marie-Therese/Westerfeld, Horst (Hrsg.) 2011: Vom Open Government zur Digitalen Agora. ISPRAT Whitepaper (Forschungskooperation „Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.). Hamburg

Kloepfer, Michael (Hrsg.) 2011: Netzneutralität in der Informationsgesellschaft. Berlin

Klüver, Reymer 2012: Wikipedia gegen Washington, in. Süddeutsche Zeitung v. 18.1.2012

Koch, Moritz 2012: Ungeniert mächtig, in: Süddeutsche Zeitung v. 19.1.2012

Koch, Moritz/Brinkmann, Bastian 2012: Das Imperium schlägt zurück, in: Süddeutsche Zeitung v. 21./22.1.2012

Krastev, Ivan 2012: Transparenz schafft kein Vertrauen, Interview in: Süddeutsche Zeitung v. 19.10.2012

Kreye, Andrian 2011: Hoffen auf das Web 3.0, in: Süddeutsche Zeitung v. 1.2.2011

Kröger, Detlef/Hanken, Claas 2003: Casebook Internetrecht, Berlin u.a.

Küchemann, Fridtjof 2012: Wartet, bis erst die Chinesen kommen, in: Frankfurter Allgemeine Zeitung v. 9.6.2012

Kurz, Constanze 2012: Die neuen Hilfssheriffs des Internets, in: Frankfurter Allgemeine Zeitung v. 11.5.2012

Kurz, Constanze/Rieger, Frank 2012: Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Frankfurt am Main

Ladeur, Karl-Heinz 2009: Neue Medien brauchen neues Medienrecht! Zur Notwendigkeit einer Anpassung des Rechts an die Internetkommunikation, in: Bieber/Eifert/Groß/Lamla, S. 23

Ladeur, Karl-Heinz 2012: Neue Institutionen für den Daten- und Persönlichkeitsschutz im Internet: „Cyber-Courts" für die Blogosphere, in: Datenschutz und Datensicherheit S. 1

Lanier, Jaron 2012: Gadget. Warum die Zukunft uns noch braucht. Berlin

Lenk, Klaus 2004: Der Staat am Draht: Electronic Government und die Zukunft der öffentlichen Verwaltung – eine Einführung. Berlin

Lewinski, Kai von 2011 a: Recht auf Internet, in: Rechtswissenschaft Heft 1, S. 70

Lewinski, Kai von 2011 b: Kodifikationsstrategien im Datenschutzrecht, oder: Wann ist der Zeitpunkt der Unkodifizierbarkeit erreicht?, in: Michael Kloepfer (Hrsg.), Gesetzgebung als wissenschaftliche Herausforderung. Gedächtnisschrift für Thilo Brandner, S. 107. Baden-Baden

Lewinski, Kai von 2012: Europäisierung des Datenschutzrechts, in: Datenschutz und Datensicherung H. 8, S. 564

Lukaßen, David 2010: Die Fallpraxis der Informationsbeauftragten und ihr Beitrag zur Entwicklung des Informationsfreiheitsrechts. Berlin

Masing, Johannes 2012 a: Ein Abschied von den Grundrechten. Die Europäische Kommission plant per Verordnung eine ausnehmend problematische Neuordnung des Datenschutzes, in: Süddeutsche Zeitung v. 9.1.2012, S. 17

Masing, Johannes 2012 b: Herausforderungen des Datenschutzes, in: Neue Juristische Wochenschrift, S. 2305

Mayer, Franz C. 2011: Die Verpflichtung auf Netzneutralität im Europarecht, in: Kloepfer (Hrsg.) 2011, S. 81

Mayer, Pavel 2011: Die Antwort der Piraten, in: Frankfurter Allgemeine Zeitung v. 17.10.2011, S. 27

Meckel, Miriam 2012: Mensch wird Maschine. Wie lange unterscheiden wir uns noch vom Computer?, in: Die Zeit Nr. 27 v. 28.6.2012, S. 13

Metzinger, Thomas 2012: Leidgenossen. Interview mit Thomas Wagner-Nagy, in: Süddeutsche Zeitung v. 21./22.7.2012, S. 20

Morozov, Evgeny 2011: The Net Delusion. How Not to Liberate the World. New York

Müller, Klaus J. 2010: Gewinnung von Verhaltensprofilen aus intelligenten Stromzählern, in: Datenschutz und Datensicherung, S. 359

Ostrom, Elinor 1999: Die Verfassung der Allmende: jenseits von Staat und Markt. Tübingen

Pariser, Eli 2011: The Filter Bubble: What the Internet Is Hiding from You. London

Passig, Kathrin/Lobo, Sascha 2012: Internet: Segen oder Fluch. Berlin

Pham, Khuê/Wefing, Heinrich 2012: Ausgeschwärmt, in: Die Zeit v. 31.10.2012, S. 3

Plotkin, Robert 2012: Computer Ethics. New York

Prantl, Heribert 2012: Acta sunt servanda, in: Süddeutsche Zeitung v. 13.2.2012

Prummer, Julia 2012: Der untreue Freund, in: Süddeutsche Zeitung v. 20.4.2012, S. 18

Rosenbach, Marcel/Stark, Holger 2011: Staatsfeind WikiLeaks. München und Hamburg

Roßnagel, Alexander 2012: Datenschutzgesetzgebung: Monopol oder Vielfalt, in: Datenschutz und Datensicherung S. 553

Roßnagel, Alexander/Jandt, Silke 2010: Datenschutzkonformes Energieinformationsnetz, in: Datenschutz und Datensicherung S. 373

Rüß, Oliver René 2001: E-democracy, in: Zeitschrift für Rechtspolitik, S. 518

Schaar, Peter 2007: Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. München

Schaar, Peter/Roth, Jürgen 2012: Quo Vadis Informationsfreiheit?, in: Dix, Alexander/Franßen, Gregor u.a. (Hrsg.), Informationsfreiheit und Informationsrecht. Jahrbuch 2011. Berlin, S. 1-18

Schoch, Friedrich 2009: Informationsfreiheitsgesetz. Kommentar. München

Schoch, Friedrich 2012: Das Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft, in: Sachs, Michael/Siekmann, Helmut (Hrsg.), Der grundrechtsgeprägte Verfassungsstaat. Festschrift für Klaus Stern zum 80. Geburtstag. Berlin, S. 1491

Schrape, Jan-Felix 2010: Neue Demokratie im Netz? Kritik an den Visionen der Informationsgesellschaft. Bielefeld

Schulz, Sönke E. 2010: Macht Art. 91 c GG E-Government-Gesetze der Länder erforderlich?, in: DÖV S. 225

Schwarz-Schilling, Carola 2011: Netzneutralität aus der Perspektive der Bundesnetzagentur, in: Kloepfer (Hrsg.) 2011, S. 133

Seckelmann, Margrit 2009: Renaissance der Gemeinschaftsaufgaben in der Föderalismusreform II?, in: DÖV S. 747

Seckelmann, Margrit/Bauer, Christian 2012: Liquid Democracy, e-Democracy und Legitimation: Zur politischen Willensbildung im Zeichen des Web 2.0, in: Hill, Hermann/Schliesky, Utz (Hrsg.), Die Vermessung des virtuellen Raums: E-Volution des Rechts- und Verwaltungssystems III. Baden-Baden, S. 327.

Seubert, Sandra 2012: Der gesellschaftliche Wert des Privaten, in: Datenschutz und Datensicherheit, Heft 2, S. 100

Seubert, Sandra/Niesen, Peter (Hrsg.) 2010: Die Grenzen des Privaten. Baden-Baden

Sieber, Ulrich 2012: Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag. München

Siemen, Birte 2006: Datenschutz als europäisches Grundrecht. Berlin

Spindler, Gerald 2012: Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung. Gutachten F zum 69. Deutschen Juristentag. München

Stephan, Felix 2012: Das Twittern im Walde: Alle reden von der Echtzeit-Demokratie – aber wollen wir das wirklich?, in: Süddeutsche Zeitung v. 26.3.2012

Trojanow, Ilija/Zeh, Juli 2009: Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte. München

Voss, Kathrin 2012: Demokratische Beteiligung per Web, www.julius-leber-forum.de/projekte/digitale-oeffentlichkeit/...

Voßkuhle, Andreas 2011: Einführung, in: Grundgesetz für die Bundesrepublik Deutschland, Beck'sche Textausgabe, 60. Auflage. München

Warren, Samuel D./Brandeis, Louis D. 1890: The Right to Privacy, in: Harvard Law Review vol. IV no. 5, 193

Weber, Christian 2012: Die Maschinen unter uns, in: Süddeutsche Zeitung v. 21./22.7.2012, S. 20

Wefing, Heinrich 2011: Neustart. Recht, Macht und Demokratie: Die Politiker müssen das Netz beherrschen, sonst beherrscht das Netz die Politik, in: Die Zeit v. 20.10.2011, S. 1

Wefing, Heinrich 2012: Einfach nur autoritär. Es wird Zeit, der Weltmacht Facebook Grenzen aufzuzeigen, in: Die Zeit v. 2.2.2012, S. 1

Wegener, Bernhard W. 2006: Der geheime Staat. Arkantradition und Informationsfreiheitsrecht. Göttingen

Weichert, Thilo 2012: Facebook, der Datenschutz und die öffentliche Sicherheit, in: Möllers, Martin H. W./van Ooyen, Robert Chr. (Hrsg.), Jahrbuch Öffentliche Sicherheit 2012/2013. Frankfurt am Main, S. 249

Weizenbaum, Joseph 1977: Die Macht der Computer und die Ohnmacht der Vernunft. Frankfurt am Main

Werle, Raymund 2000: Innovationspotenziale im Internet – Selbstregelung auf Strukturebene, in: Hoffmann-Riem, Wolfgang (Hrsg.), Innovation und Telekommunikation: Rechtliche Steuerung von Innovationsprozessen in der Telekommunikation, Baden-Baden, S. 141

Wewer, Göttrik 2012: Auf dem Weg zum gläsernen Staat? Privatsphäre und Geheimnis im digitalen Zeitalter, in: der moderne staat, H. 2/2012, S. 247

Whitman, James Q. 2004: The Two Western Cultures of Privacy: Dignity versus Liberty, in: Yale Law Journal, vol. 113, p. 1153

Wien, Andreas 2012: Internetrecht: Eine praxisorientierte Einführung. 3. Aufl. Heidelberg

Worms, Christoph/Gusy, Christoph 2012: Verfassung und Datenschutz. Das Private und das Öffentliche in der Rechtsordnung, in: Datenschutz und Datensicherheit, Heft 2, S. 92

Zielcke, Andreas 2010: Was ist privat? Europäer sehen den Datenschutz anders als Amerikaner, in: Süddeutsche Zeitung v. 4.3.2010, S. 11

Zielcke, Andreas 2012: Durchsichtig dunkel: Über die Tücken des Transparenzgebots der Piratenpartei, in: Süddeutsche Zeitung v. 29.3.2012