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.